Université de Montréal

La responsabilité des intermédiaires techniques en droit pénal canadien, à la lumière des pratiques internationales

Par
Sevgi Kelci

Faculté de droit

Mémoire présenté à la Faculté des études supérieures en vue de l'obtention du grade de
Maître en droit (L.L.M.) option Technologies de l'information

Avril 2009

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé :

La responsabilité des intermédiaires techniques en droit pénal canadien, à la lumière des pratiques internationales

présenté par :
Sevgi Kelci

A été évalué par un jury composé des personnes suivantes:

Vincent Gautrais
Président-rapporteur

Pierre Trudel
Directeur de recherche

Hugues Parent
Membre du jury

REMERCIEMENTS

Je tiens à remercier très sincèrement ma famille qui a su endurer mon long parcours universitaire. Ce mémoire n'aurait jamais pu se concrétiser sans l'aide de mon père, Ali, dont le soutient financier, l'expérience et les conseils me furent indispensables, de ma mère, Zehra, de ma sœur, Aynur et de mon frère, Vacip, dont l'écoute, le support et la confiance n'ont jamais failli. Ce travail clôture une étape importante de ma vie à laquelle a participé chacun avec ferveur et encouragements.

Je souhaiterais remercier particulièrement la personne qui m'a épaulé quotidiennement pendant la période de la rédaction, Erdal.

Je souhaiterais également prendre le temps de remercier mon directeur de recherche, le professeur Pierre Trudel, qui m'a guidé et suivi dans la réalisation de cette mission ainsi que dans l'univers fascinant de la recherche pendant 2 années. Son soutien intellectuel a permis de donner à ce projet toute sa finesse et son intérêt. Ses questions ont suscité en moi le besoin de me dépasser et de réaliser au meilleur de moi-même en requestionnant sans cesse mon argumentation qui est l'aboutissement de longues réflexions. Sans oublier mon ancien maître de stage en notariat, Me Pierre Pepin, dont la confiance en mes aptitudes, l'écoute et les conseils m'ont permis de tracer mon cheminement professionnel. Je n'aurais pas pu espérer de meilleurs mentors.

Un grand merci à vous tous.

RÉSUMÉ

La question de la responsabilité pénale des intermédiaires techniques est un enjeu central et actuel dans la réglementation du cyberespace. Non seulement les implications économiques sont énormes mais c'est tout le cadre juridique de la responsabilité pénale des intermédiaires techniques qui est en cause. Or, l'environnement Internet comporte des spécificités qui rendent difficiles l'imputation de responsabilité à l'auteur de l'activité illicite qui peut alors se retrouver hors d'atteinte ou insolvable. La poursuite des intermédiaires techniques devient alors une solution envisageable aux autorités chargées de réprimer les délits, compte tenu de l'état de leur solvabilité et dans la mesure où ils sont plus facilement identifiables. Par le fait même, ces derniers se retrouvent alors pris dans l'engrenage judiciaire pour n'avoir que facilité la commission de l'activité en question, n'ayant aucunement pris part à la réalisation de celle-ci.

L'absence dans le corpus législatif canadien d'un régime de responsabilité spécifiquement applicable aux intermédiaires techniques nous oblige à baliser les critères qui emportent leur responsabilité pénale, à partir de « *principes directeurs* » d'imputabilité se dégageant de plusieurs textes nationaux et internationaux. Dans ce contexte, le mémoire étudiera, dans un premier temps, les conditions d'ouverture de la responsabilité pénale des intermédiaires techniques en droit pénal canadien et, dans un deuxième temps, répondra à la question de savoir si le droit pénal canadien en matière d'imputabilité des intermédiaires techniques est conforme aux *principes directeurs* ressortant de normes et pratiques internationales.

MOTS-CLÉS

Responsabilité pénale, intermédiaires techniques, environnement Internet, activités illicites, technologies de l'information,

ABSTRACT

Criminal liability of technical intermediaries is a central and actual issue in the regulation of cyberspace. Not also their vast economic implications in the cyberspace are in question, but also their entire legal framework regarding criminal liability of technical intermediaries is an unresolved issue. This is because a liability allegation to the author for an illicit activity can be difficult or impossible thanks to the complex nature of cyberspace and the insolvent status of the technical intermediaries Considering their state of solvency and identification facility, taking legal actions against the technical intermediaries will be a conceivable solution to the jurists. Having implied legal proceedings, even the fact that a judicial action will be taken against them will prevent them from involving illicit activities.

Non-existence of a liability regime which is specifically applicable to the technical intermediaries in the Canadian legislative corpus makes us obligated to apply to the « *guiding principles* » of imputability which can be released from several national and international texts. In this essay, we will study, at first, the conditions of applicability of the criminal liability for the technical intermediaries with regard to Canadian Criminal Law and, in second time, will answer the following question: Is Canadian Criminal Law complied with *guiding principles* arising from International norms and practice in terms of imputability of the technical intermediaries?

KEY WORDS

Criminal Liability, technical intermediaries, Internet environment, illicit activities, information technology.

TABLE DES MATIÈRES

LISTE DES SIGLES ET ABRÉVIATIONS

Berkeley Tech. L.J	Berkeley Tech. L.J
CA	Cour d'appel
C.cr.	Code criminel
Computer L.J.	Computer Law Journal
Crim. L.J.	Criminal Law Journal
C.R.T.C.	Conseil de la radiodiffusion et des télécommunications canadiennes
Harvard J. of L. & Tech.	Harvard Journal of Law & Technology
Hastings Comm/Ent.L.J.	Hastings Communications and Entertainment Law Journal
Leg@l.TI.	Droit des technologies de l'information
Sask. R.	Saskatchewan Regiment
TGI	Tribunal de Grande instance
Villanova L. Rev.	Villanova Law Review

« Come! Come again! Whoever, whatever you may be, come!
Heathen, idolatrous or fire worshipper come!
Even if you deny your oaths a hundred times come!
Our door is the door of hope come! Come like you are! »

Mevlana Celaleddin Rumi

INTRODUCTION

La multiplication du nombre d'intermédiaires d'Internet ainsi que l'augmentation graduelle des activités s'y déroulant expose ces derniers à d'éventuelles poursuites judiciaires, forçant les juristes à s'interroger sur leur situation juridique et à clarifier davantage leur régime de responsabilité pénale. Cette réalité devient alors source de préoccupations pour les intermédiaires eux-mêmes qui se retrouvent pris dans l'engrenage judiciaire pour le simple fait d'avoir facilité la commission d'une activité illicite, sans pour autant prendre part à la réalisation de celle-ci. C'est alors que chacun d'eux ressentent le besoin d'être informé de ses devoirs et obligations.

La question de savoir à « *qui* » devrait-on imputer la responsabilité pénale pour des dommages qui résultent de la commission d'activités illicites sur le réseau Internet devient alors incontournable dans la détermination des obligations des intermédiaires d'Internet[1]. Cette question a tout son intérêt pour amorcer un travail sérieux de réflexion. L'imputation de responsabilité pénale des intermédiaires techniques est un enjeu central et actuel relatif à la réglementation du cyberespace[2]. Il faut reconnaître, à l'instar d'André Lucas, que la *« responsabilité [tant] civile [que pénale] des acteurs de l'Internet est une des questions les plus controversées du droit des réseaux numériques, qui a*

---

[1] Voir : Alain STROWEL et Nicolas IDE, « Responsabilité des intermédiaires : actualités législatives et jurisprudentielles, disponible à http://www.droit-technologie.org/2_1.asp?dossier_id=32 (visité le 23 mai 2007); Michel RACICOT, Mark S. HAYES et Alec R. SZIBBO et Pierre TRUDEL, The cyberspace is not a « No Law Land », A Study of the Issues of Liability for Content Circulating on the Internet, Ottawa, Industrie Canada, Février 1997.

Selon l'Office de la langue française, l'expression « intermédiaire » se définit comme une « personne ou un organisme qui est chargé d'assurer la communication, la transmission des échanges d'idées ou de choses entre groupements ou individus du fait qu'il se trouve situé à un point de jonction ou de passage des uns aux autres » : Office québécois de la langue française, *Le grand dictionnaire terminologique*, Recherche –intermédiaire, en ligne sur : < http://www.granddictionnaire.com > (visité le 27 janvier 2009) ; voir *infra*, note 122. À partir de cette définition, l'on peut affirmer que les « intermédiaires techniques » sont des personnes, entreprises ou organismes qui interviennent dans la chaîne de transmission de l'information circulant dans le réseau Internet à un point de jonction ou de passage des uns aux autres.

[2] Le terme « *cyberspace* » (cyberespace en français) a été introduit dans le langage par l'auteur William Gibson dans son roman « Neuromancien ». Selon l'auteur Klein, « le « *cyberespace* » est l'espace virtuel des ordinateurs tous reliés entre eux grâce à des réseaux qu'explorent les « *cybernautes* » dont les systèmes nerveux sont directement branchés sur les réseaux grâce à des réseaux grâce à une prise fixée sur leur crâne ». Gérard KLEIN, « De la cybernétique à la cyberculture », *Le Monde, télévision, radio, multimédia*, 21, 22 janvier 1996, p. 28.

donné lieu et continue de donner lieu, à un lobbying forcené. Cela est facile à comprendre. Non seulement les enjeux économiques sont énormes, mais, comme l'a noté un rapport officiel français, derrière ces enjeux, c'est toute une « éthique » du nouvel espace cybernétique qui est en cause.[3] ».

Or, il est admis que les caractéristiques de l'environnement électronique complexifient le phénomène de l'imputation de responsabilité[4]. En effet, la rapidité des interactions se déroulant sur le réseau Internet rend difficile la recherche de preuves quant aux circonstances entourant la commission d'un acte criminel sur le réseau Internet[5]. Le caractère transfrontalier et immatériel des échanges compliquent la localisation de personnes impliquées dans les infractions criminelles[6]. Néanmoins, ces caractéristiques ne devraient pas servir de justification pour exclure la responsabilité pénale des intermédiaires techniques du droit des réseaux numériques même si, par ailleurs, cet environnement se présente comme un terrain d'incertitude lorsqu'il s'agit de poser des balises claires aux règles régissant la responsabilité pénale des intermédiaires.

Le droit pénal canadien ne comporte pas de mécanismes juridiques qui régissent spécifiquement la responsabilité pénale des intermédiaires techniques. Les dispositions de la *Loi concernant le cadre juridique des technologies de l'information*[7] qui organisent leur régime de responsabilité au niveau du droit pénal provincial[8] au Québec ne s'appliquent pas lorsqu'il s'agit de déterminer la responsabilité d'un

---

[3] André LUCAS, « La responsabilité civile des acteurs de l'Internet », (2001) *Auteurs & Média*, 42-52.

[4] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », Montréal, Éditions Thémis, 1997, p. 1-15 ; Yves Poulet et Xavier THUNIS, « Droit et informatique : un mariage difficile » dans Computers and Telecommunications : Is There a Lawyer in this Room?, Namur, Éd. Story-Scientia, 1987, 3, 9.

[5] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 1-15 à 1-17.

[6] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 1-15 à 1-17.

[7] L.R.Q., c. C-1.1 (ci-après appelée : « *LCCJTI* »). La loi québécoise organise le statut juridique des documents, quelqu'en soit leur support et établit des règles précises qui sont applicables à chacun des intermédiaires techniques. Ces règles sont énoncées à l'article 22, pour la conservation et la référence à des documents, à l'article 26, pour la conservation, et aux articles 36 et 37 pour la transmission. Ces règles balisent le champ de la responsabilité civile des intermédiaires techniques et complètent les principes généraux de la responsabilité civile énoncés à l'article 1457 du *Code civil du Québec*. L.Q. 2001, c. 32.

[8] Le droit pénal provincial a pour objet de garantir l'application et l'efficacité des lois provinciales, notamment la loi québécoise, et ce, par le biais de dispositions prescrivant des peines, amendes ou pénalités puisque c'est le Parlement fédéral qui a compétence exclusive pour définir ce que constitue un crime: art. 92(15) de la *Loi constitutionnelle* de 1867, 30 & 31 Vict., R-U., c. 3 (1867) ; Peter HOGG, *Constitutional Law of Canada*, vol. 1, 3rd ed (Supplemented). Scarborough, Ont.: Carswell, 1992 ; Pierre TRUDEL, « La responsabilité des acteurs du commerce électronique », dans Vincent GAUTRAIS, Droit du commerce électronique, Montréal, Éditions Thémis, 2003, p. 610 ; *R. c. Morgentaler*, [1993] 3 R.C.S. 463; *Egan c. Canada*, [1995] 2 R.C.S. 513 ; *Irwin Toy Ltd. c. Québec (Procureur général)*, [1989] 1 R.C.S. 927.

intermédiaire pour une activité constituant une infraction au sens des lois criminelles. S'ajoutent à celles-ci le droit pénal des corporations et les nouvelles dispositions du *Code criminel* régissant la responsabilité pénale des organisations[9] qui s'appliquent de façon générale aux intermédiaires techniques pour une activité constituant une infraction au sens des lois criminelles, sans toutefois prévoir de règles spécifiques imputables à chacun des intermédiaires techniques. En l'absence de régime de responsabilité spécialement applicable aux intermédiaires techniques dans le droit pénal canadien, il est intéressant de déterminer la responsabilité pouvant être imputable à *chacun* d'eux en vertu du droit pénal canadien. Il ressort de l'analyse du droit pénal canadien portant sur la responsabilité des intermédiaires techniques qu'il est certes difficile d'attribuer une responsabilité pénale qui serait différente à chacun des intermédiaires qui participe à la transmission de l'information, à la lumière des normes canadiennes existantes. Cette difficulté découle en partie de l'inexistence d'un régime de responsabilité pénale spécifiquement applicable aux seuls intermédiaires techniques[10]. Et en l'absence de régime de responsabilité, il faut recourir aux mécanismes supplétifs afin de leur imputer une responsabilité pénale.

Dans cette perspective, se pose la question générale de recherche suivante : quelles sont les conditions d'ouverture de la responsabilité pénale des intermédiaires techniques?

Cette question se retrouve dans le corpus jurisprudentiel et doctrinal de plusieurs systèmes juridiques où il y a ambiguïté à savoir si le droit pénal national devrait prévoir un régime de responsabilité spécifiquement applicable aux intermédiaires techniques en raison des dommages causés par la commission d'activités illicites sur le réseau Internet[11]. La difficulté d'arriver à un consensus découle du fait que le choix du législateur sur le régime applicable aura un effet direct sur le droit des utilisateurs et des intermédiaires à une protection législative adéquate. Certes, si le régime de responsabilité est trop strict, les intermédiaires techniques

---

[9] *Loi modifiant le Code criminel (responsabilité pénale des organisations)*, L.R.C. c. C-46. Veuillez noter que les dispositions de ladite loi ne s'appliquent pas directement à chacun des intermédiaires techniques ci-haut mentionnés, le recours à des méthodes d'interprétation étant nécessaire.

[10] L'on verra dans ce mémoire que, contrairement au droit pénal canadien, la *Directive européenne sur le commerce électronique* (voir *infra*, note 15) et la *loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* (voir *infra*, note 16) comportent un régime de responsabilité pénale des intermédiaires techniques.

[11] Thibault VERBIEST et Étienne WÉRY, « Le droit de l'Internet et de la société de l'information », Bruxelles, Larcier, 2001, 648 p. n° 393 et ss. Ce mémoire étudiera les instruments juridiques qui sont mentionnés à la note 22.

seront portés, afin de se protéger, à censurer le contenu de l'information transmise, ce qui aura pour conséquence de mettre en jeu le droit à la liberté d'expression. En revanche, si le régime juridique prévoit une exonération de responsabilité, ces derniers ne seront pas incités à prendre des mesures raisonnables afin de faire cesser les activités illicites se déroulant sur le réseau Internet, ce qui aura pour conséquence de compromettre les droits des utilisateurs.

Les tenants[12] de la thèse préconisant un régime d'exonération de responsabilité soutiennent que le rôle de plusieurs intermédiaires étant purement technique, leur imposer une obligation de contrôle sur le contenu de l'information transmise par leurs installations irait à l'encontre du bon sens puisque la plupart de ces acteurs –tels que les FSI, le prestataire qui fait le *caching* et le moteur de recherche– n'exercent aucun contrôle sur l'information. À l'inverse, les tenants de la thèse inverse, celle préconisant un régime de responsabilité pour les intermédiaires techniques, font valoir que ces derniers choisissent de diffuser des informations dont le contenu peut s'avérer préjudiciable à autrui. Si les intermédiaires exercent un contrôle sur une activité posant ces risques, il est difficile de voir au nom de quoi ils peuvent réclamer une immunité. Le postulat derrière cette thèse est que les intermédiaires, étant responsables de la diffusion de l'information, doivent répondre du risque qui est intimement lié à la transmission de l'information sur un territoire du réseau Internet[13].

Comme l'indique l'auteur Michel Vivant, il est possible de trouver un juste milieu entre ces deux perspectives se situant à l'extrême opposé l'une de l'autre : « *[L]'irresponsabilité de principe est inadmissible non seulement d'un point de vue juridique mais encore d'un point de vue éthique comme sociétal. Mais la responsabilité « mécanique », « par défaut » pour la raison qu'il faut trouver un responsable, et lors même que le présumé responsable n'en pourrait mais, l'est tout autant.*[14].

Pour ce dernier, l'équilibre pourrait être atteint par la création d'un régime pouvant assurer à la fois la protection des utilisateurs et des intermédiaires. De plus, ce régime devrait éviter de créer des situations où les intermédiaires pourraient être tentés

---

[12] *ibid.*

[13] Pierre TRUDEL, « La responsabilité sur Internet », juillet 2002, *Revue Droit & Toile* ; Michel VIVANT, « La responsabilité des intermédiaires de l'Internet », J.C.P. éd. G.1999. I. 180.

[14] Michel VIVANT, « La responsabilité des intermédiaires de l'Internet », *loc. cit.*, note 13.

de censurer l'information de façon à empêcher la circulation effective de l'information ou à limiter excessivement le droit à la liberté de l'expression.

C'est dans cette optique qu'il faut comprendre les deux approches législatives choisies par des acteurs étatiques et non étatiques qui visent à appréhender le problème de l'incertitude juridique relative au régime de responsabilité pénale des intermédiaires techniques. La première approche consiste à formuler une série de principes généraux traitant de la responsabilité dans son ensemble (approche horizontale). La deuxième approche consiste à traiter de manière différente la responsabilité des intermédiaires techniques en tenant compte des spécificités de chaque domaine concerné (approche verticale). L'approche horizontale a été retenue par les législateurs européens, français et québécois dans la *Directive sur le commerce électronique*[15], la *Loi pour la confiance dans l'économie numérique*[16] et dans la *Loi concernant le cadre juridique des technologies de l'information*[17]. L'approche verticale a été choisie par le législateur américain dans le *Digital Millennium Copyright Act (*DMCA) et dans la *Convention sur la cybercriminalité*[18].

Bien que ces deux approches proviennent de deux traditions juridiques différentes, il faut néanmoins souligner que l'appréciation de la responsabilité pénale des intermédiaires techniques se fait en tenant compte des trois mêmes critères et ce,

---

[15] Directive *2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur* (ci-après citée « *Directive sur le commerce électronique* »), *J.O.C.E*, n° L 178 du 17/07/2000, p. 0001 – 0016, en ligne sur : < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:FR:HTML > (visité le 2 juillet 2007). Il est à remarquer que les dispositions qui traitent des différentes activités exercées par les intermédiaires s'appliquent indépendamment du type de droits auxquels la communication en ligne est susceptible de porter atteinte. En ce sens, l'approche préconisée est une approche dite horizontale parce qu'elle consiste à prendre des mesures à effet général ou horizontal s'appliquant à toutes les formes d'atteintes à des droits subjectifs.

[16] *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, publiée au journal officiel de la République française n° 143 du 22 juin 2004 (ci-après appelée : *LCEN* ») ; Wikipédia, « Loi pour la confiance dans l'économie numérique », en ligne sur : < http://fr.wikipedia.org/wiki/Loi_sur_la_confiance_dans_l'%C3%A9conomie_num%C3%A9rique > (visité le 23 juillet 2007).

[17] *Précitée*, note 7.

[18] *Digital Millenium Copyright Act*, Pub. L. No. 105-304, 112 Stat. 2860 (1998) en ligne sur: < http://www.eff.org/IP/DMCA/hr2281_dmca_law_19981020_pl105-304.html > (visité le 2 juillet 2007). Cette loi ne fera toutefois pas l'objet de notre étude, *le Communications Decency Act* (ci-après appelé : « *CDA* »), étant plus pertinent à notre sujet : *Telecommunications Act* de 1996, Pub. L. No. 104-104, tit. V, 110 Stat. 56, 133-43 (1996) (codifié dans les sections de 47 U.S.C.). Le *CDA* est situé dans le titre V du *Telecommunications Act* de 1996, qui est amendé par le *Communications Act* de 1934. Contrairement à la *Directive sur le commerce électronique*, la *Convention sur la cybercriminalité* privilégie une approche qui consiste à énoncer un régime de responsabilité applicable également entre tous les intermédiaires techniques mais selon le type d'activités commises sur Internet. Cette principale différence avec la Convention se comprend en considérant que celle-ci constitue tout d'abord un instrument de répression pénale alors que la *Directive sur le commerce électronique* se veut un instrument de droit communautaire.

dans les deux approches : le contrôle, la connaissance et l'absence d'obligation légale de surveillance. En effet, la possibilité de mettre en cause les intermédiaires techniques suppose essentiellement que l'on puisse identifier les personnes qui ont la maîtrise de l'information diffusée dans divers environnements électroniques. Le niveau de contrôle exercé par une personne ou une entité sur l'information dans une situation donnée serait donc un facteur pertinent servant à déterminer le niveau de responsabilité imputable à cette personne, comme l'indiquent les auteurs Trudel et Schlachter[19]. Mais il importe également de tenir compte du niveau de connaissance qu'une personne détient sur le caractère dommageable de l'information pour ceux qui participent à la transmission de l'information. Par conséquent, les principes de contrôle, de connaissance et de l'absence légale de surveillance illicite serviront à titre de lignes directrices permettant de déterminer les facteurs à considérer dans l'appréciation du niveau de responsabilité imputable aux intermédiaires techniques, en l'absence de dispositions expresses prévues dans le droit pénal canadien à cet effet[20].

Même si le législateur canadien a décidé de ne pas légiférer pour un régime de responsabilité pénale qui serait spécifiquement applicable aux intermédiaires techniques, ne pourrait-on pas tout de même affirmer que le droit pénal est conforme aux principes se dégageant des normes et pratiques internationales en matière d'imputabilité?

Dans cette perspective, il paraît opportun de se poser la question spécifique de recherche suivante : quelle est la conformité des règles du droit pénal canadien régissant la responsabilité pénale des intermédiaires techniques avec les principes qui ressortent des normes et pratiques internationales? [21]

Cette question s'inscrit dans la question générale de recherche et vise à déterminer si le droit canadien est conforme aux pratiques internationales en matière de responsabilité pénale des intermédiaires techniques.

---

[19] Pierre TRUDEL, « La responsabilité des acteurs du commerce électronique », *loc. cit.*, note 8 ; Eric SCHLACHTER, « Cyberspace, The Free Market and the Free Marketplace of Ideas : Recognizing Legal Differences in Computer Board Functions », (1993) 16 *Hastings Comm/Ent.L.J.*, 113 et ss.

[20] Ce qui sera réalisé par l'analyse des textes de lois susmentionnées ainsi que par l'examen de la mise en application de ces lois devant les tribunaux nationaux et internationaux traitant de ces trois principes précédemment mentionnés.

[21] Ce travail étudiera les principes de connaissance, de contrôle et de l'absence légale de surveillance qui se dégagent de plusieurs textes nationaux et internationaux qui sont mentionnés à la note 22.

L'appréciation de l'adéquation des règles pénales canadiennes avec les pratiques internationales se fera en deux parties. La première partie présentera l'environnement Internet et ses caractéristiques ainsi que la notion d'intermédiaires techniques. La deuxième partie traitera dans son premier chapitre, des principes de contrôle, de connaissance et de l'absence d'obligation légale de surveillance comme les principaux principes d'imputabilité régissant les intermédiaires techniques, à partir d'une étude fondée sur le droit de différentes législations et des pratiques internationales[22]. Dans ce contexte, il faudra décrire brièvement les aspects généraux des instruments juridiques qui seront examinés dans ce mémoire.

Tout d'abord, ce travail étudiera la *Convention sur la cybercriminalité*[23] qui est le premier instrument international destiné à lutter contre les infractions pénales commises sur les réseaux informatiques, en réponse au problème lié à l'augmentation de la criminalité dans le cyberespace[24]. La Convention a pour but d'harmoniser l'équilibre entre d'une part, les intérêts de l'action répressive et d'autre part, le respect des droits de l'homme fondamentaux, tels que garantis par plusieurs instruments internationaux[25]. Elle vise globalement à édifier un cadre juridique universel de droit pénal destiné à combattre la « *cybercriminalité* » en fournissant au droit pénal national des mécanismes procéduraux nécessaires à la sanction des personnes coupables et de canaliser les efforts sur une gestion rapide et efficace de la coopération internationale.

---

[22] Ce mémoire étudiera les instruments juridiques suivants : a) *Convention sur la cybercriminalité*, STE n° : 185, Budapest, 23 novembre 2001 et *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, STE n°: 185, Strasbourg, 28 janvier 2003; b) Directive *2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur, supra*, note 15; c) *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, supra*, note 16; e) *Loi concernant le cadre juridique des technologies de l'information, supra*, note 7; d) *Communications Decency Act, supra*, note 18.

[23] *ibid.* La *Convention sur la cybercriminalité, loc .cit*, note 22. Elle fût adoptée le 8 novembre 2001 et le texte international est pleinement entré en vigueur le 18 mars 2004. 42 États ont signé la Convention dont le Canada qui était parmi les pays non membres. Mais seuls 14 États ont procédé à sa ratification, y excluant le Canada : Amélie M. WEBER, *Annual Review of Law and Technology: VIII. Foreign & International Law: A. Cyberlaw: Cybercrime: The Council of Europe's Convention on Cybercrime*, (2003) 18 BERKELEY TECH. L.J., p. 430.

[24] Selon la conclusion du rapport établie par le Professeur H.W.K. Kaspersen, à la demande du Comité européen pour les problèmes criminels (CDPC) et une conclusion analogue figure dans la Recommandation n° R (89) et la Recommandation n° R (95) 13 : *Convention sur la cybercriminalité*, Rapport explicatif, par. 10, STE n° : 185, Budapest, 23 novembre 2001, Conseil de l'Europe, http://www.libertysecurity.org/IMG/pdf/ExplanatoryReportFr.pdf (visité le 22 mars 2009).

[25] Notamment la *Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe*, Rome, 4 novembre 1950, R.T.E. n°5, 213 R.T.N.U. 222 ; le *Pacte international relatif aux droits civils et politiques des Nations Unies* adopté et ouvert à la signature, à la ratification et à l'adhésion par résolution de l'Assemblée générale n° 2200A (XXI) du 16 décembre 1966, R.T.C. 1976, n° 47, RTNU, vol. 999, n° 171 et d'autres conventions internationales applicables en matière de droits de l'homme qui affirment le droit à la liberté d'expression et le droit au respect de la vie privée.

La Convention fixe une norme minimale commune permettant de regrouper en quatre catégories les infractions pénales[26] qui doivent être intégrées dans le droit interne des États conformément à leurs législations nationales.

Deuxièmement, l'on examinera le Protocole[27] qui est annexé au texte principal et qui a pour vocation de compléter la Convention[28]. Le protocole énonce une série d'infractions visant l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Il vise donc à apporter une certaine précision et complémentarité au texte principal.

Troisièmement, l'on analysera la *Directive sur le commerce électronique*[29] qui vise à créer un cadre juridique cohérent à l'échelon européen pour le commerce électronique et à faciliter l'essor de la société de l'information[30]. L'approche adoptée par le texte européen consiste à éviter les conséquences d'une surréglementation, en se fondant sur les libertés du marché intérieur, en prenant en considération les réalités

---

[26] Les quatre catégories d'infractions sont les suivantes : a) les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes : accès illégal, interception illégale, atteinte à l'intégrité des données, atteinte à l'intégrité du système, abus de dispositifs; b) les infractions informatiques : falsification et fraude informatiques; c) les infractions se rapportant au contenu : actes de production, diffusion, possession de pornographie enfantine Un protocole additionnel devrait inclure la propagation d'idées racistes et la xénophobie à travers les réseaux. et d) les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes : la distribution à grande échelle de copies illégales d'œuvres protégées etc.

[27] *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, STE n°: 185, Strasbourg, 28 janvier 2003. Malgré les maintes objections qui ont précédé la mise en place d'une infrastructure de lutte contre la discrimination raciale et la xénophobie, notamment en raison de la préoccupation que nourrissait certains pays dont les États-Unis sur les risques d'atteintes au droit à la liberté d'expression, un protocole distinct a tout de même été adopté. Les États-Unis ont invoqué des atteintes au droit à la liberté de l'expression, notamment le premier amendement à la Constitution : Conseil de l'Europe, *Le secrétaire général du Conseil de l'Europe : « Le but est d'harmoniser les législations pénales »*, http://www.coe.int/t/f/com/dossiers/interviews/20020309_InterviewSGLiberation.asp#P11_996 (visité le 10 juillet 2007).
Le protocole a été adopté le 28 janvier 2003. Le Canada a signé le Protocole le 8 juillet 2005 et l'entrée en vigueur du protocole nécessite 5 ratifications. À l'heure actuelle, 4 États l'ont ratifié : Ministère de la Justice du Canada, *Le Canada signe une entente internationale en vue de lutter contre les crimes racistes sur Internet*, 8 juillet 2005, http://www.justice.gc.ca/fra/nouv-news/cp-nr/2005/doc_31572.html (visité le 10 juillet 2007). 27

[28] Le protocole a un caractère obligatoire et chaque État doit adopter une législation appropriée visant l'incrimination des actes de nature raciste et xénophobe commis par le biais de systèmes informatiques et assurer la mise en œuvre adéquate des infractions dans leur législation interne : *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, Rapport explicatif, par. 8-9, STE n°: 185, Strasbourg, 28 janvier 2003, Conseil de l'Europe, http://www.inach.net/content/cctreatyaddexfr.html (visité le 22 mars 2009).

[29] Directive *2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur* (ci-après citée « *Directive sur le commerce électronique* »), *J.O.C.E*, n° L 178 du 17/07/2000, p. 0001 – 0016, en ligne sur : < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:FR:HTML > (visité le 2 juillet 2007).

[30] Définition donnée au Considérant 17 de la *Directive sur le commerce électronique* et l'article 2 (a) qui renvoie au paragraphe 2 de l'article 1er de la *Directive n°98/34/CE relative au mécanisme de transparence réglementaire* telle que modifiée par la *Directive n°98/48/CE* ; Europa, Activités de l'Union européenne –Synthèse de la législation, « Aspects juridiques du commerce électronique (« directive sur le commerce électronique ») », en ligne sur : < http://europa.eu/scadplus/leg/fr/lvb/l24204.htm > (visité le 18 juillet 2007).

commerciales et en assurant une protection efficace des objectifs d'intérêt général[31]. Elle a également comme objectif d'éliminer les disparités dans la jurisprudence des États membres de façon à promouvoir la sécurité et la confiance au sein du commerce électronique[32]. Par ailleurs, la *Directive sur le commerce électronique* encourage l'émergence des codes de conduites, le règlement extrajudiciaire des différends, en appliquant les principes d'indépendance, de transparence, du contradictoire, de l'efficacité de la procédure, de la légalité de la décision, de la liberté des parties et de représentation[33], ainsi que la coopération entre les États membres[34]. Ces derniers doivent s'assurer que les sanctions qu'ils adoptent soient « *effectives, proportionnées et dissuasives* »[35]. Le champ d'application de la *Directive sur le commerce électronique* couvre tous les services de la société de l'information, tels que les services entre entreprises (B2B), les services entre entreprises et consommateurs (B2C), les services qui sont gratuitement fournis aux consommateurs, tels que les journaux en ligne, les services financiers en ligne, la publicité et les services permettant des transactions électroniques en ligne[36]. Elle s'applique exclusivement aux prestataires de services établis au sein de l'Union européenne[37].

Quatrièmement, l'on étudiera la *loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*[38] qui a comme objectif de favoriser le développement du commerce électronique, en clarifiant le droit applicable aux services de l'Internet. Elle donne une définition claire de la notion de communication[39] et de commerce électronique et précise l'ensemble des dispositions qui sont rattachées à

---

[31] Europa, Activités de l'Union européenne –Synthèse de la législation, « Aspects juridiques du commerce électronique (« directive sur le commerce électronique ») », *loc. cit.*, note 30.
[32] *ibid.*
[33] En vertu de l'article 17 de la *Directive sur le commerce électronique.*
[34] Voir les articles 16 à 19 de la *Directive sur le commerce électronique.*
[35] Voir article 20 de la *Directive sur le commerce électronique.*
[36] *ibid.*
[37] En vertu de l'article 3 de la *Directive sur le commerce électronique* qui énonce ce qui suit : « Chaque État membre veille à ce que les services de la société de l'information fournis par un prestataire établi sur son territoire respectent les dispositions nationales applicables dans cet État membre relevant du domaine coordonné ». Les prestataires de services peuvent consister en des opérateurs de sites Web ou les transmetteurs ou les prestataires qui offrent des services de *caching* : en vertu des articles 14, 12 et 13 de la *Directive sur le commerce électronique.*
[38] *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, publiée au journal officiel de la République française n° 143 du 22 juin 2004 (ci-après appelée : *LCEN* ») ; Wikipédia, « Loi pour la confiance dans l'économie numérique », en ligne sur : < http://fr.wikipedia.org/wiki/Loi_sur_la_confiance_dans_l'%C3%A9conomie_num%C3%A9rique > (visité le 23 juillet 2007).
[39] On entend par communication au public en ligne : « toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur : article 1 de la Loi.

l'utilisation et au développement de l'Internet dans la sphère publique[40]. Elle fournit un ensemble de mesures réglementaires en ce qui a trait à la responsabilité des prestataires de services, tout en s'attardant à maintenir un équilibre entre la liberté de l'expression et la protection des droits individuels[41].

Enfin, ce mémoire analysera le *Communications Decency Act*[42] qui institue un régime d'immunité en faveur de l'utilisateur d'un service informatique interactif pour la transmission, l'envoi et la publication d'un « *offensive material* »[43] par les services d'Internet. Il faut noter que l'étendue de la loi se limite aux sanctions civiles et pénales. Le champ d'application de cette loi exclut donc toutes enfreintes aux lois criminelles ou à la propriété intellectuelle (article 230 (d)), ce à quoi remédiera en partie le *Digital Millenium Copyright Act.*

Dans le deuxième chapitre, l'on examinera la conformité des règles du droit pénal canadien aux principes antérieurement identifiés. Étant donné que le droit pénal canadien ne comporte aucun régime spécifique en la matière et que le droit découlant de différentes législations et de pratiques internationales[44] prévoit un régime de responsabilité qui lui est propre, il est utile de faire des comparaisons avec ces instruments juridiques[45] afin de dégager les mécanismes d'imputabilité s'y trouvant. Cette conformité sera vérifiée par l'application des mécanismes d'imputabilité du droit pénal canadien à l'égard de chacun des intermédiaires techniques. Dans l'étude de cette section, il faut alors se demander si les règles du droit pénal en matière de responsabilité donnent lieu à une appréciation *complète* de la responsabilité pénale des intermédiaires concernés, à partir de ces trois principes[46]. Cette analyse servira à répondre aux questions générale et spécifique de recherche et permettra de fixer les

---

[40] *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, loc. cit.*, note 16.
[41] *ibid.*
[42] *Telecommunications Act* de 1996, Pub. L. No. 104-104, tit. V, 110 Stat. 56, 133-43 (1996) (codifié dans les sections de 47 U.S.C.).
[43] Par « *offensive material* », il faut comprendre les contenus « *obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable* » : article 230 (c)(1).
[44] Voir les législations mentionnées à la note 22. Cette étude ne vise aucunement à prétendre que le droit interne de différentes législations et la pratique internationale sont « plus » ou « moins » efficaces que le droit pénal canadien. L'on reconnaît seulement que la raison pour laquelle le législateur étranger a choisi de légiférer doit présupposer l'existence d'un minimum d'efficacité (effets voulus par le législateur, soit la sanction d'activités illicites) en ces règles qui sont spécifiquement applicables aux intermédiaires techniques.
[45] Voir les législations mentionnées à la note 22.
[46] En d'autres mots, les règles pénales canadiennes produisent-elles les effets voulus par le législateur, soit la sanction d'activités illicites. Le recours à des méthodes interprétatives se fera par une lecture des textes de lois pertinents et à partir d'une analyse de la jurisprudence et doctrine pertinentes.

paramètres des conditions d'ouverture de la responsabilité pénale des intermédiaires techniques.

La réflexion sur la responsabilité pénale des intermédiaires techniques est importante pour plusieurs motifs. Tout d'abord, en fournissant des balises juridiques sur lesquelles se fonde leur responsabilité pénale, il sera possible d'obtenir condamnation d'un acte grave qui est commis sur Internet. Puisqu'il va de l'intérêt public de punir des actes graves, tels que la pornographie juvénile, la fraude informatique, la contrefaçon, l'utilisation non autorisée des données ou des services d'un système informatique, la falsification des données informatiques ou la transmission de virus informatiques, etc. Or, il est admis que cette éventuelle condamnation peut s'avérer pratiquement impossible si l'on considère que la personne qui est à l'origine de cet acte illicite est souvent difficilement identifiable ou peut souvent se retrouver hors d'atteinte en raison de l'architecture de l'Internet[47]. Quoi que les intermédiaires techniques n'en soient pas l'auteur principal de l'activité en question, il demeure qu'en se tournant vers ces derniers, l'« *activité* » en question s'en trouverait sanctionnée. En outre, en connaissant mieux les conditions d'ouverture de leur responsabilité pénale, les intermédiaires techniques seront en mesure de prendre des moyens concrets afin de se prémunir contre d'éventuels recours en responsabilité pénale.

L'on commencera alors l'étude du sujet en introduisant l'environnement Internet et ses caractéristiques.

TITRE I– LES INTERMÉDIAIRES D'INTERNET

Dans le titre premier titre, il convient, en premier lieu, de présenter l'environnement Internet et ses caractéristiques dans une perspective qui tient compte de ses effets sur l'imputation de responsabilité des intermédiaires techniques et en deuxième lieu, de définir de façon non exhaustive la notion d'« intermédiaires techniques » afin de mettre en contexte la problématique de départ.

---

[47] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 5-13 ; Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », en ligne sur : < http://www.chairelrwilson.ca/documents/TRUDEL_resp_internet.pdf> (visité le 5 janvier 2009) ; Pierre TRUDEL, « La responsabilité des acteurs du commerce électronique », *loc. cit.*, note 8, p. 609.

CHAPITRE I– L'environnement Internet et ses caractéristiques au regard de la responsabilité pénale des intermédiaires techniques

Le cyberespace fait indiscutablement partie de la vie quotidienne des canadiens comme ailleurs. Un bon nombre d'individus naviguent sur le cyberespace afin de s'adonner à diverses activités alors que plusieurs « scientifiques » réfléchissent à l'impact qu'il engendre sur le droit, notamment sur la responsabilité des intermédiaires techniques. Il ne suffit pas de prendre pour acte cette réalité qui est devenue en quelque sorte banale pour tirer les conclusions qui s'imposent. Il faut plutôt prendre le temps d'expliquer en quoi elle consiste et de présenter ses principales caractéristiques pour ensuite asseoir un raisonnement.

Dans ce contexte, il y a lieu, dans ce premier chapitre, de présenter l'environnement Internet et ses caractéristiques pour deux motifs. Premièrement, la question de la responsabilité pénale des intermédiaires techniques ne peut se poser sans l'avoir préalablement situé dans cet environnement qui est le cyberespace. Deuxièmement, les caractéristiques du cyberespace ont des conséquences sur le régime de la responsabilité des intermédiaires techniques.

Section I– L'environnement Internet et ses caractéristiques

Dans cette section, il y a lieu, tout d'abord, de cerner la notion de cyberespace afin de bien comprendre l'objet de notre étude avant de décrire, par la suite, les caractéristiques de cet environnement virtuel qui est le cyberespace.

A) Le cyberespace

Dans ce premier paragraphe, il conviendra de circonscrire la notion de cyberespace qui constitue une étape obligée afin de comprendre ses différentes particularités.

Le terme « cyberespace » qui a été introduit dans le langage par William Gibson[48] signifie de nos jours un « *lieu imaginaire appliqué métaphoriquement au réseau*

[48] William GIBSON, « Neuromancer », New York, Ace Books, 1984.

Internet et dans lequel les internautes qui y naviguent s'adonnent à des activités diverses »[49]. Le cyberespace est parfois utilisé dans le sens de « monde virtuel »[50].

Le concept de cyberespace se rattache également à l'univers numérique constitué d'interconnections de réseaux d'ordinateurs dont en particulier le réseau Internet. Comme infrastructure qui est à la base du cyberespace se trouve alors Internet. Selon le Multi dictionnaire de la langue française, Internet se définit comme étant un « *[r]éseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés, qui sont reliés par le protocole de communication TCP-IP*[51] *et qui coopèrent dans le but d'offrir une interface unique à leurs utilisateurs* »[52]. Il s'annonce donc comme une plate-forme mondiale de communication qui permet la circulation de l'information, en faisant abstraction des frontières territoriales et en échappant à l'exercice d'un contrôle centralisateur[53]. Il permet aux usagers de communiquer entre eux, notamment par le biais de courriels, de messageries ou par le biais de groupes de discussion. Comme autre utilité, Internet offre aux usagers la possibilité de circuler dans le cyberespace pour obtenir de l'information à propos d'un sujet donné, pour flâner et parfois même pour commettre un délit, comme dans le monde réel. Ces derniers peuvent alors décider du contenu de l'information qu'ils diffusent sur Internet. Les intermédiaires, quant à eux, servent de conduit pour assurer l'acheminement de cette information.

Le cyberespace se rapporte donc à un environnement virtuel dans lequel circule l'information via le réseau Internet qui est alors considéré comme un moyen de communication permettant aux usagers de décider de ce qu'ils envoient et donnant la possibilité aux intermédiaires d'assurer l'acheminement de l'information. Dans ce contexte, il s'annonce donc comme un *environnement humain et technologique qui est le siège d'événements ayant des conséquences juridiques*[54] à l'endroit de ceux qui décident de l'information et à l'égard de ceux qui n'en décident pas.

---

[49] Office québécois de la langue française, *Le grand dictionnaire terminologique*, Recherche –cyberespace, en ligne sur : < http://www.granddictionnaire.com > (visité le 27 janvier 2009).
[50] *ibid.*
[51] Transmission Control Protocol et Internet Protocol.
[52] Marie-Éva DE VILLERS, « Multi dictionnaire de la langue française », 3e éd., Montréal, Québec Amérique, 1997, p. 802.
[53] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 1-15.
[54] Office québécois de la langue française, *Le grand dictionnaire terminologique*, Recherche –cyberespace, en ligne sur : < http://www.granddictionnaire.com > (visité le 27 janvier 2009).

Après avoir parcouru la notion de cyberespace, il convient de décrire quelques particularités de cet environnement qui est le cyberespace.

B) Les caractéristiques du cyberespace

Dans ce paragraphe, il y a lieu de décrire les principales caractéristiques qui gouvernent le cyberespace puisque comme l'on verra dans la deuxième section de ce premier chapitre, elles ont des effets sur le régime de la responsabilité pénale des intermédiaires techniques.

Les caractéristiques du cyberespace ont été rapportées dans une décision américaine, à savoir *American Civil Liberties Union* v.*Reno*[55]. Dans ce contexte, il conviendra de présenter succinctement celles qui ont des effets sur la responsabilité des intermédiaires techniques[56], à savoir l'interactivité, l'ubiquité et la délocalisation ainsi que la dématérialisation.

i) L'interactivité

En premier lieu, il faut relever le caractère interactif des communications effectuées par les usagers et transmises par les intermédiaires techniques dans le réseau Internet.

Selon la définition proposée par l'auteur Sylvette Guillemard, l'interactivité désigne « le fait que des gestes, des actes se répondent et alternent »[57]. Ainsi, la vidéoconférence ou le clavardage constituent deux exemples de situations permettant à deux ou plusieurs personnes d'interagir sur Internet, chaque participant pouvant jouer

---

[55] *Reno, Attorney General of the United States, et al.* v. *American Civil Liberties Union (ACLU) et al.*, 117 S.Ct. 2329, 138 L.Ed.2d 874 (1997), en ligne sur : < http://supct.law.cornell.edu/supct/html/96-511.ZO.html > (visité le 16 février 2009) ; Lucie HOUDE, « Internet et le paradigme juridictionnel », Mémoire de maîtrise, Faculté des études supérieures, Université de Montréal, Québec, juin 2003, p. 12, 13 : « 1° Internet est un réseau de réseaux. 2° Certains réseaux sont fermés, non liés à d'autres, mais beaucoup sont reliés à des réseaux qui permettent à chaque ordinateur de chaque réseau de communiquer avec les autres ordinateurs des autres réseaux. 3° Internet a été conçu pour faire en sorte que les liens entre les ordinateurs et les réseaux d'ordinateurs soient effectués sans l'intervention humaine ou contrôle humain, ayant l'habilité de rediriger automatiquement l'information si l'un ou l'autre des liens manquait ou n'était pas disponible: c'est ce que l'on appelle le routage. C'est l'une des raisons pour lesquelles Internet est difficilement contrôlable. 4° Les messages et parties de messages échangés entre les ordinateurs ne suivent pas tous le même chemin sur le réseau: Internet utilise des protocoles qui permettent de subdiviser les messages en « paquets » plus petits, lesquels se promènent indépendamment sur le réseau, et parviennent tous à la même destination, mais pas nécessairement en même temps ».

[56] L'on verra dans la section II les raisons pour lesquelles ces caractéristiques ont des effets sur la responsabilité des intermédiaires techniques.

[57] Sylvette GUILLEMARD, « Le droit international privé face au contrat de vente cyberspatial », Thèse de doctorat, Faculté des études supérieures, Université Laval, Québec, janvier 2003, p. 226.

un rôle actif dans la communication de l'information. À cet égard, l'auteur Trudel et son équipe mentionnent ce qui suit : « *[l]es communications "en ligne" sont interactives en ce sens qu'elles permettent aux usagers de retrouver l'information qu'ils désirent et de choisir les types de communications dans lesquels ils veulent s'engager* »[58].

Cette explication de l'interactivité sur Internet permet de suggérer que l'usager a une certaine marge de manœuvre tant dans la cueillette d'informations que dans d'autres activités. Ainsi, ce dernier peut consulter un nombre indéfini de pages Web et décider du contenu de l'information qu'il s'apprête à diffuser. Il se retrouve alors dans une situation où il devient « acteur et producteur d'informations »[59] dans la mesure où, tout comme celui qui décide, il a la faculté de décider du contenu de l'information ainsi que du type d'activité qu'il désire exercer sur Internet. En revanche, cette démonstration permet également de constater que l'intermédiaire technique ne joue qu'un rôle passif puisque n'intervenant que lors de la transmission de l'information. Le rôle de ce dernier est plutôt comparable à celui du participant qui ne décide pas du contenu de l'information.

Il faut admettre que les outils assurant les communications dans le cyberespace donnent lieu à des interactions plus nombreuses, plus faciles et plus rapides entre les usagers et les intermédiaires[60]. Ainsi, un usager peut demander au blogueur de modifier un type d'informations figurant sur son blogue, pour le motif qu'il s'agit d'une information fausse ou inexacte. Le blogueur peut alors acquiescer à sa demande et faire la modification à l'intérieur de quelques minutes. Des usagers peuvent s'inscrire sur un site de rencontre virtuelle en remplissant le formulaire prévu à cet effet. Le maître du site peut alors faire suite à leur demande. L'on constate que les fonctionnalités techniques de l'Internet permettent ainsi aux participants de modifier rapidement les informations de départ. Grâce à cette interactivité, les activités se déroulant sur Internet revêtent une dimension plus dynamique que dans le monde réel.

---

[58] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 1-9.
[59] *ibid.*
[60] Sylvette GUILLEMARD, « Le droit international privé face au contrat de vente cyberspatial », *loc. cit.*, note 57, p. 227.

Par conséquent, l'on peut affirmer que c'est au niveau de son ampleur ou l'accélération du phénomène[61] que l'interactivité prend sa coloration dans le monde virtuel.

L'interactivité peut occasionner des difficultés en matière de preuve. Ainsi, la quantité d'informations qui transigent sur le réseau à l'intérieur d'un court laps de temps peut engendrer la perte de données transmises entre les participants de la communication. L'établissement de la preuve entourant les circonstances de cette activité devient alors difficile ou quasi-impossible. Faute d'établir les éléments constitutifs d'une infraction imputable à l'auteur du crime, les autorités se tourneront alors vers les intermédiaires, étant donné qu'ils sont plus facilement identifiables[62].

Par conséquent, l'interactivité rend difficile la recherche de preuves entourant les circonstances de l'activité illicite, ce qui rend possible la poursuite des intermédiaires.

ii) L'ubiquité et la délocalisation

En deuxième lieu, il convient de traiter des caractéristiques du cyberespace qui sont liées à l'ubiquité et à la délocalisation.

L'ubiquité se rapporte à la « *possibilité d'être présent en plusieurs lieux à la fois* »[63]. Dans l'environnement Internet, l'ubiquité se rattache au fait qu'une même information puisse être disponible en même temps à plusieurs points du réseau Internet. Ainsi, l'information publiée par un blogueur peut se trouver de façon simultanée au Canada et au Japon. Cette situation est comparable à la télévision dans la mesure où les téléspectateurs, tout comme les usagers, peuvent accéder en même temps à des informations identiques. L'ubiquité implique également le fait pour les usagers de pouvoir modifier simultanément l'information en question. Ainsi, plusieurs usagers peuvent se rendre sur le site de *Wikipédia*[64] et modifier en même temps l'information s'y trouvant.

---

[61] Sylvette GUILLEMARD, « Le droit international privé face au contrat de vente cyberspatial », *loc. cit.*, note 57, p. 228.

[62] Les intermédiaires techniques possèdent une adresse IP propre et constante alors que les usagers utilisent une adresse IP différente à chaque session, c'est-à-dire à chaque branchement. À cet égard, voir, *supra*, p. 17.

[63] *ibid.*

[64] Voir *infra* la section II du chapitre II de ce mémoire.

Dans l'environnement Internet, cette notion d'ubiquité se rattache intimement à celle de la délocalisation[65]. Le fait qu'une information soit accessible à partir de plusieurs *endroits* du réseau suppose qu'elle soit disponible en même temps dans le cyberespace. L'information circule partout, sans que l'on puisse déterminer de façon précise cet *endroit*. La transmission de l'information s'effectue alors sur plusieurs *endroits* du réseau, en faisant abstraction de frontières terrestres[66]. Ainsi, les notions de lieu physique et de frontières se bousculent dans le cyberespace et les activités s'y déroulent de manière « déterritorialisées »[67].

Dans le cyberespace, la localisation est déterminée par le système en fonction de l'adresse IP de l'usager. Ainsi, l'information transmise par un usager ne provient pas de Japon mais de 123.456.78.55 et elle ne parvient pas au Canada mais à 897.543.45.77. De plus, il faut savoir que les usagers individuels n'ont pas d'adresse IP fixe[68]. C'est par le biais de leur fournisseur de services Internet qu'ils en obtiennent une, lorsqu'ils lui en font la demande, c'est-à-dire lors de chaque session[69]. Ainsi, à chaque branchement, l'usager a une nouvelle identification. Par contre, les intermédiaires techniques qui prennent souvent la forme d'entreprises, d'administrateurs ou d'institutions possèdent une adresse IP propre et constante[70].

Les particularités du cyberespace liées à l'ubiquité et à la délocalisation compliquent l'identification et la localisation des personnes ayant commis l'activité illicite[71]. Si l'information se trouve disponible simultanément et à partir de plusieurs endroits du cyberespace, c'est que plusieurs usagers peuvent y accéder en même temps et la modifier à leur guise. Comme l'usager possède une identification différente à chaque branchement, il devient alors difficile d'identifier et de localiser celui qui est à

---

[65] Sylvette GUILLEMARD, « Le droit international privé face au contrat de vente cyberspatial », *loc. cit.*, note 57, p. 231.
[66] Sylvette GUILLEMARD, « Le droit international privé face au contrat de vente cyberspatial », *loc. cit.*, note 57, p. 231.
[67] *ibid.*
[68] *ibid*, 222.
[69] *ibid*, 222.
[70] *ibid*, 222.
[71] À cet égard, voir l'affaire *Yahoo!* qui démontre bien les difficultés qui sont liées à la localisation et au « découpage » géographique du cyberespace : *Yahoo (UEJF et Licra* c. *Yahoo ! Inc. et Yahoo France*, TGI Paris, réf., 22 mai 2000, Comm. com. électr.2000. comm. n°92, note J-Chr. GALLOUX ou en ligne : Revue du droit des technologies de l'information < http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm> (visité le 8 juin 2007).

l'origine de l'information litigieuse[72]. Comme solution à ce problème, l'on opte pour la poursuite des intermédiaires qui sont beaucoup plus facilement identifiables puisqu'ils possèdent une adresse IP constante.

Par conséquent, l'ubiquité et la délocalisation rendent difficiles l'imputation d'une responsabilité à l'auteur du crime et, par le fait même, ouvrent la porte à la possibilité de poursuivre les intermédiaires techniques.

iii) La dématérialisation

En troisième lieu, il convient de traiter de la particularité du cyberespace qui est liée à la dématérialisation.

Le terme « dématérialisation » signifie « *le processus par lequel la manipulation de papier est supprimée* »[73]. Dans l'environnement Internet, les nombreux biens qui étaient connus sous la forme matérielle et palpable deviennent intangibles. Ainsi, l'on peut penser aux documents, aux œuvres musicales et cinématographiques. Ce qui signifie qu'il n'y a plus d'écrit sur support papier. En outre, les « activités illicites » qui sont commises dans le monde réel deviennent également dématérialisées dans le cyberespace. Ainsi, l'on peut penser aux activités, telles que la possession de la pornographie juvénile, l'interception illégale des données.

L'absence de tangibilité comporte de nombreux avantages, notamment rapidité, souplesse et facilité d'accès[74]. Toutefois, elle présente plusieurs inconvénients, plus particulièrement en matière de preuve[75]. L'information diffusée par l'usager étant sous la forme dématérialisée dans le cyberespace, l'on convient que le contenu de cette information peut disparaître, sans laisser de traces. Par ailleurs, une activité illicite peut être commise par un usager, sans que l'on puisse établir les circonstances entourant la commission de cette activité. Par conséquent, les personnes qui sont à l'origine de

---

[72] Il est à noter qu'il est possible de retracer l'adresse IP de l'usager puisque le fournisseur d'accès a les moyens d'accéder à des informations le concernant. Toutefois, l'intermédiaire n'a généralement que peu de renseignements à propos de l'usager en question. Selon la pratique habituellement observée au Québec, les renseignements que l'abonné fournit à son fournisseur de service sont réduits au strict minimum, aucune identification officielle n'étant exigée : Sylvette GUILLEMARD, « Le droit international privé face au contrat de vente cyberspatial », *loc. cit.*, note 57, p. 222.

[73] Conseil National du crédit et du titre, « Problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres », Paris, Banque de France, 1997, p. 11.

[74] Sylvette GUILLEMARD, « Le droit international privé face au contrat de vente cyberspatial », *loc. cit.*, note 57, p. 235.

[75] À cet égard, l'on peut d'ailleurs observer plusieurs initiatives législatives qui ont été prises tant à l'échelle nationale qu'internationale. Voir, la *Loi concernant le cadre juridique des technologies de l'information*, *précitée*, note 7 ; la *Directive sur le commerce électronique*, *précitée*, note 15.

l'activité illicite peuvent se trouver hors d'atteinte. Ce qui amènera les autorités à envisager des poursuites contre les intermédiaires, étant donné qu'ils sont beaucoup plus facilement accessibles.

Dans cette perspective, la dématérialisation rend difficile la poursuite des personnes qui sont l'auteur de l'activité litigieuse, ce qui accroît par le fait même, la tentative d'exposer les intermédiaires techniques à des poursuites judiciaires.

Après avoir parcouru la notion de cyberespace ainsi que ses principales caractéristiques, l'on peut faire les constats suivants. Le cyberespace se décrit comme un environnement dans lequel siègent les interactions qui impliquent des conséquences juridiques à l'endroit des intermédiaires d'Internet[76]. Il présente des particularités qui peuvent rendre difficiles l'imputation de responsabilité à l'auteur du crime. L'interactivité des communications peut causer la perte de données. L'ubiquité et la délocalisation compliquent l'identification ainsi que la localisation de la personne responsable. La dématérialisation confère un caractère évanescent aux informations qui sont transmises via Internet. Par conséquent, les autorités chargés de réprimer les délits peuvent être tentées de se tourner vers les intermédiaires techniques afin d'obtenir justice, étant donné qu'ils sont beaucoup plus facilement identifiables.

En conclusion, le cyberespace et ses caractéristiques ont des incidences sur la responsabilité pénale des intermédiaires techniques.

Section II– Les conséquences des caractéristiques du cyberespace sur la responsabilité pénale des intermédiaires techniques

L'examen des caractéristiques du cyberespace a permis de constater qu'elles avaient des incidences sur la responsabilité pénale des intermédiaires techniques. Dans cette perspective, il convient alors, dans cette section, de dégager ces principales conséquences qui sont de trois ordres, à savoir la difficulté d'identifier les personnes, de les localiser et la difficulté de rechercher des preuves entourant les circonstances d'un crime.

---

[76] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4. p. 1-15 ; Yves Poulet et Xavier THUNIS, « Droit et informatique : un mariage difficile » *loc. cit.*, note 4, 3, 9.

A) L'identification des personnes

En premier lieu, il convient d'étudier l'un des principaux effets des caractéristiques du cyberespace, à savoir la difficulté d'identifier les personnes qui sont responsables dans la commission d'un crime.

L'identification des personnes est une opération cruciale dans l'environnement virtuel, tout comme dans le monde réel d'ailleurs. Elle fait directement référence à l'identité d'une personne dont le concept peut évoluer avec la société. Dans notre société, ce concept se rattache à une série d'obligations à respecter ou des droits à faire valoir. Dans le monde réel, l'on fait appel à des mécanismes d'identification afin de s'assurer de l'identité d'une personne. Alors que dans le monde virtuel, l'on doit développer des mécanismes qui sont encore plus sophistiqués afin de s'assurer de l'identité des parties dans le contexte d'un environnement dématérialisé et délocalisé. Ainsi, dans une transaction qui implique des millions de dollars, la confirmation de l'identité est essentielle. C'est alors que l'on voit se développer de plus en plus des mécanismes d'identification et de certification[77].

En revanche, certaines particularités du cyberespace, comme la possibilité pour l'usager de ne pas dévoiler son identité et la situation de l'anonymat[78], font échec à l'identification de l'usager. Grâce aux techniques assurant l'anonymat sur Internet[79], diverses activités illicites deviennent plus faciles à commettre, telles que la diffusion de matériel raciste et xénophobe, la fraude informatique, la falsification de données mais également plus difficiles à contrôler. Il est possible de demander aux fournisseurs de services Internet (FSI) de dévoiler le nom de ces usagers mais ces intermédiaires sont généralement réticents à le faire, étant donné que ce n'est pas à eux d'assumer une telle responsabilité. Il devient alors pratiquement impossible de retracer ces usagers anonymes en passant par les FSI. Toutefois, si un juge ordonne à l'intermédiaire en question de collaborer afin de retracer l'auteur de l'activité litigieuse, il sera alors tenu

---

[77] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 19-23 à 19-31.

[78] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 11-59.

[79] L'on peut penser à des logiciels qui permettent à un usager d'envoyer des courriels sans dévoiler son identité (par exemple par *Mixmaster (obscura.com)* et *anonymisers.com.* Le serveur enlève alors du courriel transmis les données permettant d'identifier l'expéditeur.

de dévoiler l'identité de ce dernier[80]. Toutefois, comme mentionné dans la section qui traite des caractéristiques du cyberespace, ces informations ne sont réduites qu'au strict minimum, étant donné qu'aucune identification officielle de l'abonné n'est exigée selon la pratique habituellement établie au Québec[81].

Comme les personnes responsables de l'activité illicitement commise sur Internet sont difficilement identifiables en raison de certaines caractéristiques de l'Internet, même avec l'aide du FSI, il devient concevable de se tourner vers les intermédiaires qui s'annoncent comme étant plus facilement identifiables. Rappelons que ces derniers possèdent une adresse IP propre et constante.

Par conséquent, le cyberespace rend ardue l'identification des personnes qui sont à l'origine de l'activité illicite ainsi que l'imputation d'une responsabilité pénale à leur endroit[82], ce qui accroît, par le fait même, la tentative d'exposer les intermédiaires techniques à d'éventuelles poursuites en responsabilité.

B) La localisation des personnes

En deuxième lieu, il convient d'examiner une autre conséquence découlant des caractéristiques du cyberespace, à savoir la difficulté de localiser les personnes.

La difficulté de localiser les personnes qui commettent des activités illicites sur Internet s'ajoute à celle qui est liée à l'identification des personnes. La cause de cette difficulté réside dans le mode de fonctionnement du réseau Internet. L'adresse IP d'un usager ne correspond pas toujours à sa localisation physique puisque, comme mentionné précédemment, ce dernier peut obtenir une nouvelle adresse IP à chaque branchement[83]. Ainsi, comme il y a une absence de lien systématique entre une adresse IP et un lieu géographique donné[84], il peut devenir difficile de connaître avec certitude la localisation de l'usager.

---

[80] L'article 27 de la *Loi concernant le cadre juridique des technologies de l'information, précitée*, note 7 , prévoit que le fournisseur de services Internet agissant à titre d'intermédiaire technique ne doit pas empêcher « [l]es autorités responsables d'exercer leurs fonctions, conformément à la loi, relativement à la sécurité publique ou à la prévention, à la détection, à la preuve ou à la poursuite d'infractions ».

[81] Voir, *supra*, note, 72. À notre avis, étant donné que les FSI se rattachent à une juridiction donnée, il serait intéressant de leur demander l'identité de l'usager afin de déterminer la juridiction dans laquelle il se trouve.

[82] *ibid.*

[83] Voir, *supra*, p. 17.

[84] James P. DONOHUE, « Litigation in Cyberspace: Jurisdiction and Choice of Law –A United States Perspective », *American Bar Association, Subcommittee on International Transactions* (1997), 7.

Toutefois, il faut tout de même préciser que, grâce à l'émergence de nouvelles technologies de localisation[85] qui permettent à certaines entreprises de cibler des zones géographiques où elles souhaitent faire affaires, il y a une atténuation du problème lié à la localisation des personnes. Ainsi, cette technologie pourrait permettre de mieux cibler les personnes qui entrent dans la juridiction d'un État donné[86]. Ce qui permettrait de retracer la personne qui a commis l'activité illicite.

Même si ces nouvelles technologies peuvent en quelque sorte alléger le niveau de difficulté, il demeure que les particularités du cyberespace rendent ardue la localisation des personnes qui ont commis l'activité litigieuse dans le réseau Internet. Ainsi, en raison de l'interactivité des communications s'y déroulant, un même usager peut se retrouver dans différents *endroits* du réseau. En raison de l'ubiquité des communications, plusieurs usagers peuvent se retrouver en même temps dans un même lieu et modifier les informations figurant à cet *endroit*.

Par conséquent, l'imputation d'une responsabilité pénale à l'auteur du crime devient difficile pour les autorités qui optent alors pour la poursuite des intermédiaires, étant donné qu'ils sont plus facilement identifiables

C) La recherche de preuves entourant les circonstances d'une activité illicite

En dernier lieu, l'on traitera de la difficulté de rechercher des preuves entourant les circonstances d'une activité illicite comme dernière conséquence découlant des particularités du cyberespace.

L'établissement des circonstances entourant la commission d'une activité illicite constitue une étape obligée pour imputer une responsabilité pénale à son auteur[87]. Dans le cyberespace, reconstituer les faits permettant de relier l'activité illicite à son auteur devient difficile à cause de la dématérialisation des

---

[85] Patrimoine canadien, « Le Web sémantique – d'un « Web de pages » à un « Web de données », en ligne sur : < http://www.rcip.gc.ca/Francais/Contenu_Numerique/web_semantique/index.html > (visité le 16 avril 2009). L'on y mentionne deux importantes technologies existantes, le langage XML *(Extensible Markup à Language)* et le RDF *(Resource Description Framework),* lesquelles permettent d'agencer et d'utiliser les informations qui circulent sur le Web de façon plus intelligente, par exemple dans les domaines de la localisation, de l'identification, en utilisant entre autres des agents intelligents, c'est ce que l'on appelle « le Web sémantique ».

[86] Lucie HOUDE, « Internet et le paradigme juridictionnel », *loc. cit*, note 55, p. 19.

[87] *Canada (Citoyenneté et Immigration)* c. *Khosa*, 2009 CSC 12 (CanLII).

communications s'y déroulant[88]. Ainsi, si l'activité ne laisse aucune trace tangible, il devient quasi-impossible de rétablir les faits qui sont à la base de l'activité illicite. Au surplus de quoi la rapidité avec laquelle se déroulent les communications sur Internet et le caractère éphémère des informations circulant dans cet environnement favorisent la disparition de preuves visant les circonstances de cette activité[89]. Il s'ensuit qu'il devient difficile de rattacher avec certitude la commission d'une activité illicite à son auteur. Face à l'impossibilité d'imputer cette responsabilité pénale, les autorités peuvent être tentées de se tourner vers les intermédiaires techniques qui s'avèrent beaucoup plus faciles d'accès.

Par conséquent, les caractéristiques du cyberespace ont pour effet de compliquer la recherche de preuves entourant les circonstances d'une activité illicite. Il s'ensuit une difficulté d'imputer une responsabilité pénale à son auteur et une possibilité d'exposer les intermédiaires à d'éventuelles poursuites en responsabilité.

Après avoir analysé les conséquences des particularités du cyberespace sur la responsabilité des intermédiaires techniques, l'on peut faire les constats suivants. Le cyberespace comporte des spécificités qui ont un impact sur la responsabilité des intermédiaires. Le mode de fonctionnement du cyberespace et la situation de l'anonymat freinent l'identification des personnes. L'immatérialité, l'ubiquité et caractère international des interactions compliquent la localisation des personnes. La rapidité des interactions, la volatilité et l'absence de tangibilité des données engendrent des problèmes de preuves entourant les circonstances de la commission d'une activité illicite.

Par conséquent, l'imputation d'une responsabilité pénale à l'auteur de l'activité devient ardue pour les autorités en raison des spécificités du médium qui s'avèrent comme un terrain fertile à la poursuite des intermédiaires techniques.

Après avoir présenté l'environnement Internet ainsi que ses caractéristiques au regard de leur responsabilité pénale, il convient dès lors de parcourir la notion d'intermédiaires techniques qui constitue l'objet de notre dissertation.

---

[88] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 1-15. Dans le cyberespace, l'on assiste à une redéfinition des coordonnées spatio-temporelles en raison du changement rapide dans les rôles et les lieux de l'environnement Internet alors que dans le monde réel, ces coordonnées sont relativement stables : *ibid.*

[89] *ibid.*

CHAPITRE II- La notion d'« intermédiaires techniques »

Dans le premier chapitre, l'on a présenté l'environnement Internet et ses caractéristiques afin de mettre en contexte l'objet de notre dissertation qui est la notion d'intermédiaires techniques en rapport avec le régime de responsabilité qui leur est applicable. L'on a constaté que l'auteur de l'activité illicite pouvait, en raison des spécificités du médium, se retrouver hors d'atteinte pour ainsi éviter toute condamnation éventuelle. La poursuite des intermédiaires techniques a paru aux autorités comme une solution envisageable, étant donné qu'ils sont plus facilement identifiables. Les intermédiaires techniques se sont retrouvés exposés à des poursuites judiciaires pour n'avoir que facilité la commission de l'activité en question, n'ayant aucunement participé à la réalisation de celle-ci. Ce qui a amené les juristes à réfléchir sur l'état de leurs devoirs et responsabilités dans une situation donnée. Or, les critères permettant d'engager leur responsabilité se fondent sur les rôles joués par chacun dans la chaîne de communication de l'information. Afin de bien comprendre les règles juridiques encadrant leur responsabilité, il faut arriver à expliquer ce que fait un intermédiaire technique.

Les rôles joués par chacun dans la chaîne de communication seront décrits à partir d'une analyse métaphorique, soit un procédé linguistique se caractérisant par l'analogie qui permet de procurer des solutions juridiques qui existent à l'égard de la chose à laquelle le phénomène nouveau est analogue[90]. Le droit de la responsabilité des intermédiaires techniques intègre les devoirs et obligations de chacun en fonction du rôle occupé par chacun. Il s'organise sur la base de métaphores qui tient compte « *des différences et similitudes entre les régimes développés qui présentent des analogies avec la communication dans les réseaux électroniques ouverts tels que le transport par chemin de fer ou la diffusion d'imprimés* »[91]. Le recours à des analogies permettra de situer le rôle joué par chacun et de saisir la portée des règles actuelles régissant leur régime de

---

[90] Pierre TRUDEL « Les responsabilités dans le cyberespace », *supra*, note 91, p. 242 ; Pierre TRUDEL, « La responsabilité sur Internet », *loc. cit*, note 13, p. 20.

[91] Pierre TRUDEL « Les responsabilités dans le cyberespace » dans Les dimensions internationales du droit du cyberespace, collection Droit du cyberespace, Paris, Éditions UNESCO- Économica, 2000, p. 240 ; Pierre TRUDEL et R. GÉRIN-LAJOIE, « La protection des droits et des valeurs dans la gestion des réseaux ouverts » dans : Centre de recherche en droit public (CRDP), Les autoroutes électroniques : usages, droit et promesses, Montréal, Éditions Yvon Blais, 1995, p. 279, p. 306-307; David R. JOHNSON and Kevin MARKS, « Mapping Electronic Data Communications Onto Existing Legal Metaphors : Should We Let Our Conscience (and our Contracts) Be our Guide? », (1993) 38 *Villanova L. Rev.* 487-515.

responsabilité. Toutefois, ce procédé comporte des limites qu'il convient d'expliquer. L'avènement des environnements électroniques a fait en sorte que le débat portant sur « *le vide juridique* » à l'égard d'Internet s'est alimenté avec l'absence de consensus sur les métaphores devant servir à expliquer les rôles des participants à la communication[92]. Par conséquent, comme l'indique Professeur Trudel, il est recommandé de ne pas trop généraliser « *à partir d'un type de réglementation aux environnements électroniques sur la seule base de ressemblance qu'ils peuvent présenter avec des environnements préexistants* »[93]. Il faut donc reconnaître qu'en raison des spécificités propres aux environnements électroniques, ce ne sont pas toutes les situations qui sont susceptibles d'extrapolation à partir des caractéristiques que présentent les environnements préexistants.

Malgré les limites qui sont rattachées au procédé métaphorique, il servira tout de même à dégager les ressemblances et différences se présentant dans les rôles de chacun des intervenants dans la communication électronique, notamment les opérateurs du réseau, les fournisseurs d'information, les transporteurs de l'information, etc.[94]. D'où l'intérêt de circonscrire la notion d'intermédiaires techniques au moyen d'une échelle d'intensité qui s'établit en fonction du degré de contrôle exercé par l'intervenant sur l'activité illicite. Dans ce contexte, il faut commencer, dans un premier temps, par ceux qui exercent un degré de contrôle élevé, à savoir l'éditeur et le diffuseur et poursuivre, dans un deuxième temps, par les acteurs qui n'en exercent *a priori* pas, à savoir l'hébergeur, celui qui fournit des services de référencement, celui qui fait le stockage de l'information (le *caching*) et le transmetteur.

Section I- Ceux qui décident

Afin de bien cerner la notion d'intermédiaires techniques, il faut connaître les acteurs qui ne sont pas des intermédiaires, c'est-à-dire ceux qui décident du caractère litigieux de l'information ou activité et ceux qui se placent au début de l'échelle de contrôle. D'où l'intérêt de définir dans cette section, la notion d'éditeur et de diffuseur, c'est-à-dire les acteurs qui sont à l'origine de l'activité litigieuse.

---

[92] Pierre TRUDEL « Les responsabilités dans le cyberespace », *supra*, note 91, p. 242.
[93] *ibid.*, p. 242 ; R.M. NEUSTADT, G.P. SKALL and M. HAMMER, « The regulation of electronic publishing », *Federal Communications Law Journal*, n° 33, 1981, p. 331-332.
[94] Pierre TRUDEL « Les responsabilités dans le cyberespace », *supra*, note 91, p. 242.

Ceux qui sont à l'origine de l'information circulant dans l'environnement Internet relèvent de cette catégorie d'acteurs. Il s'agit de personnes, entreprises ou organismes qui exercent un contrôle effectif sur le contenu de l'information qu'ils diffusent. Si ces derniers détiennent le pouvoir discrétionnaire de publier telle ou telle information, c'est qu'ils ont connaissance du contenu de l'information. Sur le plan de la responsabilité pénale, la personne qui choisit de mettre en ligne l'information doit assumer la responsabilité qui découle de son caractère illicite ou défectueux. Ce principe ressort également de la loi québécoise[95]. Outre l'auteur du message, l'éditeur et le diffuseur sont les premiers à répondre de l'acte fautif qu'ils posent dans le cyberespace. Commençons tout d'abord par l'éditeur.

A) L'éditeur

L'éditeur est celui qui publie l'information. La publication implique un acte positif de son auteur qui suppose une connaissance de la teneur de l'information transmise[96]. Comme l'indique le Professeur Trudel, « *dans les environnements électroniques, publier de l'information peut résulter de la transmission de fichiers, de discussions dans le cadre de conférences électroniques, de l'envoi d'un courriel ou encore de la mise à disposition d'informations dans des fichiers pouvant être transférés via le réseau* »[97]. Ainsi, la loi française définit l'éditeur comme *une personne qui détermine les contenus qui doivent être mis à la disposition du public sur le service qu'elle a créé ou dont elle a la charge*[98].

La liberté éditoriale se traduit par le pouvoir qu'exerce un acteur d'Internet sur le contenu de l'information. Lorsqu'il se réserve le droit de n'acheminer que les informations qu'il juge conformes à ses politiques, il exerce son pouvoir de contrôle sur le contenu de l'information, c'est-à-dire qu'il choisit d'exercer sa liberté éditoriale. De ce pouvoir de contrôle découle la responsabilité de l'acteur pour la diffusion de l'information délictueuse[99]. Et il encourt une très lourde responsabilité dans la mesure

---

[95] *Supra*, note 7.
[96] Loftus E. BECKER Jr., « The Liability of Computer Bulletin Board Operators for Demation Posted by Others », (1989) 22 *Conn. L. Rev.* 203-239, 217.
[97] Pierre TRUDEL, « La responsabilité des acteurs du commerce électronique » *loc. cit.*, note 8, p. 612.
[98] La définition de l'éditeur est énoncée dans la décision *Jean-Yves Lafesse* c. *Dailymotion*, TGI de Paris, 3ème chambre, 1ère section, 15 avril 2008, en ligne sur : <http://www.juriscom.net/jpt/visu.php?ID=1057 > (visité le 2 mars 2009) qui rapporte l'article 6-3-1 de la *LCEN*.
[99] *ibid.*

où il est tenu pour être au courant que l'information délictueuse est susceptible de causer des dommages à autrui. À titre d'exemple, dans l'affaire *Stratton Oakmont Inc.* c. *Prodigy Services Co.*[100], le tribunal a déclaré Prodigy responsable des dommages causés à des tiers en soutenant qu'il assumait le rôle d'éditeur. Les faits donnant ouverture à la responsabilité de Prodigy sont simples. Un abonné de Prodigy a envoyé un message diffamatoire concernant le président de Stratton à partir du babillard électronique du réseau[101]. Prodigy pouvait par le biais d'un logiciel censurer toute information ne répondant pas au critère qu'il avait annoncé dans sa publicité, soit le service « *familial* », afin de s'assurer que les messages qu'il reçoit soient conformes à sa politique. La Cour a qualifié Prodigy d'éditeur, estimant qu'il avait une maîtrise du contenu de l'information qui était diffusée dans son babillard électronique puisqu'il avait la faculté de restreindre les messages pouvant s'avérer dommageables et qu'il était par conséquent, supposé de connaître la présence du message diffamatoire. Par le manquement à son obligation de supprimer le message délictueux, il se rend responsable du dommage subi par la tierce victime.

Dans cette décision, la Cour a conclu que lorsqu'un maître de site déclare qu'il offre un type de service exclusif dénué de tous vices, qu'il adopte une politique du site, qu'il met en place des mesures techniques destinées à faire respecter ladite politique et qu'il prévoit une procédure de résolution des conflits, il devient alors responsable des gestes fautifs posés par l'intermédiaire de son serveur[102]. D'autres s'opposent à ce constat, en déclarant que le fait d'avoir la faculté de choisir le genre de littérature qu'il veut offrir ne fait pas de lui un éditeur[103]. Toutefois, il faut rejoindre l'approche qui constate l'existence d'un contrôle éditorial lorsqu'un intervenant à la communication maîtrise le contenu de la transmission et lorsqu'il a le pouvoir de supprimer les messages qui ne répondent pas à des critères qu'il détermine d'avance[104].

---

[100] *Stratton Oakmont, Inc.* v. *Prodigy Services Co.*, 23 Med L.R. 1794 (N.Y. Sup. Ct. 1995).
[101] Pierre TRUDEL, « La responsabilité des acteurs du commerce électronique », *loc. cit.*, note 8, p. 613.
[102] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 5-5 ; David LOUNDY, « Holding the line, on-line, expands liability », (8 juin 1995) *Chicago Daily Law Bulletin* 6.
[103] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 5-6.
[104] *ibid.* Dans l'affaire *Cubby*, la Cour reconnaît que le rôle d'un opérateur de babillards électroniques est comparable à celui d'un éditeur lorsque ce dernier a procédé à la vérification du message préalablement à sa communication au public : *Stratton Oakmont, Inc.* v. *Prodigy Services Co.*, *précitée*, note 100.

La décision précitée témoigne de l'importance par les tribunaux de tenir compte du degré de contrôle exercé par le maître du site sur le contenu de l'information afin de définir son rôle. Or, l'on assiste aujourd'hui à une certaine tendance par les tribunaux à recourir à des critères qui ne s'inscrivent pas dans les textes de lois[105]. L'on observe ainsi un courant jurisprudentiel qui se fonde sur le rôle joué par le maître du site dans la configuration de celui-ci et conséquemment, du niveau d'implication éditoriale pouvant en découler[106]. À cet égard, le TGI de Paris a qualifié le maître du site *MySpace* d'éditeur, considérant que les fonctions occupées par celui-ci dépassaient celles d'un simple hébergeur, tout en admettant toutefois que les fonctions qu'il exerce sont celles d'un fournisseur d'hébergement[107]. Dans ce sens, la Cour a estimé que : « *[en] imposant une structure de présentation par cadres, qu'elle met manifestement à la disposition des hébergés et diffusant, à l'occasion de chaque consultation, des publicités dont elle tire manifestement profit, elle a le statut d'éditeur et doit en assumer les responsabilités* ».

Dans l'affaire *Olivier Martinez*[108], le TGI de Paris qui reprend le critère lié à la mise en disposition du site a qualifié le site *Fuzz* d'éditeur, estimant que le maître du site en question avait effectué un choix éditorial en « *renvoyant au site celebrites-stars.blogspot.co, [...] en agençant différentes rubriques telles que celles intitulées « People » et en titrant en gros caractères « Kylie Minogue et Olivier Martinez toujours amoureux ensemble à Paris* ». Or, *Fuzz* n'avait pas eu la possibilité de filtrer cette information, étant donné que ce site était organisé selon une structure de présentation permettant la diffusion automatique de l'information fournie par les internautes. Le Tribunal a jugé que *Fuzz* devait supporter une responsabilité éditoriale du fait de la publication de l'information litigieuse, même en dépit du fait qu'il ne pouvait *maîtriser* le contenu de

---

[105] *Doe* c. *MySpace*, No. 1:06-cv-00983-SS (W.D. Tex 2007) ; *Jean-Yves L. dit LAFESSE / Myspace*, TGI Paris, Ordonnance de référé 22 juin 2007, en ligne sur : Legalis.net, < http://www.legalis.net/jurisprudence-decision.php3?id_article=1965 > (visité le 21 janvier 2009) ; Julien TAÏEB, « Prestataires techniques de l'Internet : le sens des responsabilités », Juriscom.net, en ligne sur : < http://www.juriscom.net/pro/visu.php?ID=1066 > (visité le 22 janvier 2009).

[106] *Doe* c. *MySpace*, *précitée*, note 105 ; *Jean-Yves L. dit LAFESSE / Myspace*, *précitée*, note 105 ; Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit.*, note 47, p. 15.

[107] *Doe* c. *MySpace*, *précitée*, note 105 ; *Jean-Yves L. dit LAFESSE / Myspace*, *précitée*, note 105.

[108] *Olivier Martinez* c./ *Bloobox Net*, TGI Paris, référé, 26 mars 2008, Juriscom.net, en ligne sur : http://www.juriscom.net/jpt/visu.php?ID=1043 (visité le 22 janvier 2009). Dans cette décision, *Fuzz* qui est un site permettant aux utilisateurs d'Internet de poster de l'information par le biais de sa plate-forme et de les partager ailleurs sur Internet a été poursuivi par l'acteur Olivier Martinez pour atteinte à sa vie privée.

celle-ci. Dans les deux autres décisions dont les faits sont similaires[109], le TGI de Nanterre se base sur ce même critère pour qualifier les maîtres des sites *Lespipoles* et *Dico du Net* d'éditeurs. Bien qu'il soit minoritaire, ce courant jurisprudentiel est à l'effet que lorsque l'agencement des flux RSS est substantiellement contrôlé par ces derniers, il en découle une implication éditoriale[110] qui engage la responsabilité de ces derniers quant au contenu.

En conclusion, les tribunaux se montrent enclins à invoquer de nouveaux critères afin d'appliquer le statut d'éditeur aux maîtres des sites communautaires alors qu'il est manifeste que le courant majoritaire est à l'effet contraire[111]. L'on assiste ainsi à une ambiguïté de la notion d'éditeur. Par conséquent, le critère de contrôle sur le contenu de l'information s'avère incomplet et mal défini par les tribunaux conduisant ainsi à des décisions contradictoires[112].

Après avoir fait un survol sur la notion d'éditeur, faisons le même exercice pour celle de diffuseur.

B) Le diffuseur

Les diffuseurs sont assujettis aux mêmes standards de responsabilité que les éditeurs[113]. La responsabilité civile s'applique à la presse écrite, à la radio et à la télévision, sauf si les dispositions d'une loi en suspendent ou en modifient l'application[114].

Le diffuseur est responsable du fait des personnes qui interviennent en leur propre nom dans la transmission de propos dommageables. La règle applicable au

---

[109] *M. O. D. c/ SARL Planète Soft*, TGI Nanterre, 7 mars 2008, décision, Juriscom.net, en ligne sur : http://www.juriscom.net/jpt/visu.php?ID=1035 (visité le 22 janvier 2009) ; *M. Olivier Dahan c/* M. *Eric Duperrin*, TGI Nanterre, 28 février 2008, Juriscom.net, en ligne sur : http://www.juriscom.net/jpt/visu.php?ID=1031 (visité le 22 janvier 2009). Dans ces décisions, un réalisateur français avait reproché aux maîtres des sites *Lespipoles, Dico du Net* de publier un flux RSS dont le contenu portait atteinte à la vie privée et qui renvoyait à un article mis en ligne sur le site de *Gala.fr*.

[110] *ibid.*

[111] Comme l'on verra dans la section portant sur la définition de l'hébergeur. Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit.*, note 47, p. 15.

[112] *Doe* c. *MySpace*, *précitée*, note 105 ; *Jean-Yves L. dit LAFESSE / Myspace*, *précitée*, note 105 ; *Olivier Martinez* c./ *Bloobox Net*, *précitée*, note 108 ; *M. O. D. c/ SARL Planète Soft*, *précitée*, note 109 ; *M. Olivier Dahan c/* M. *Eric Duperrin*, *précitée*, note 109 ; Julien TAÏEB, « Prestataires techniques de l'Internet : le sens des responsabilités », *loc. cit*, note 105.

[113] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 5-7.

[114] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 5-7.

Québec en matière de responsabilité stipule que même lorsqu'il est établi que ce dernier a pris tous les moyens raisonnables afin de prévenir la diffusion des propos dommageables, il demeure tout de même responsable des dommages qui sont causés à des tiers[115]. À cet effet, cette règle juridique se rapproche d'un certain courant jurisprudentiel français qui considère que, même si la responsabilité ne résulte pas directement des propos formulés par une personne du public qui sont retransmis « *en direct* » au public, elle s'ensuit de l'« *autorisation* » que le diffuseur donne à cette personne[116]. Ainsi, la responsabilité du diffuseur sera engagée du fait des propos dommageables dès lors qu'il les endosse ou bien qu'il montre une certaine connivence[117].

Le diffuseur n'est toutefois pas en mesure de vérifier le caractère dommageable des propos qui sont diffusés au public. Dans ce sens, il y a lieu de faire référence à l'opérateur de la presse (pour un journal), du courrier qui transporte la publication ou des ingénieurs radio ou télé[118]. S'il ne connaît pas le contenu de l'information, il est peu probable qu'il puisse prévenir les propos s'avérant dommageables au public.

Par conséquent, le régime de responsabilité qu'on lui impute ressemble à celui qui est attribuable à un transporteur, c'est-à-dire qu'il n'est pas tenu de répondre du contenu dommageable des messages qu'il transmet[119]. Toutefois, il y a une nuance à apporter à cette règle : lorsque le diffuseur connaît ou s'il y a des motifs sérieux de croire qu'il aurait une connaissance effective du contenu diffamatoire qui est transmis, il sera tenu responsable du dommage qui en résulte[120].

Il est possible de constater que l'éditeur[121] et le diffuseur exercent un certain niveau de contrôle sur le contenu de l'information véhiculée dans les réseaux.

---

[115] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 5-7 ; Pierre TRUDEL et France ABRAN, « Droit de la radio et de la télévision », Montréal, Éditions Thémis, 1991, p. 464.

[116] *Affaire Polac*, TGI Paris, 29 janvier 1986, D. 1986, flash n° 10.

[117] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 5-7.

[118] David J. LOUNDY, « E-LAW 4: Computer Information Systems Law and System Operator Liability », (1998) 21 *Seattle University Law Review* 1075 ; Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 5-7.

[119] Terri A. CUTRERA, « Computer Networks, Libel and the First Amendment », (1992) 11 *Computer L.J.* 555-583; Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 5-7.

[120] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 5-7.

[121] L'éditeur est sans aucun doute celui qui se place au début de l'échelle de contrôle, soit avant le diffuseur.

Lorsqu'ils « *autorisent* » une personne du public à émettre l'information litigieuse, ils agissent en tant que décideur et se voient par conséquent imputer la responsabilité qui en découle. Le critère de contrôle étant l'un des facteurs à considérer, il y a une certaine tendance dans la jurisprudence française qui tient également compte du rôle joué par le maître du site Web dans la configuration de celui-ci pour qualifier un tel acteur d'éditeur. Malgré cette nuance, le lien entre le rôle joué par l'acteur d'Internet et l'imputation de sa responsabilité est irréfutable. Après avoir présenté les décideurs de l'information litigieuse, examinons maintenant ceux qui, *a priori*, n'en décident pas.

Section II- Ceux qui ne décident pas

Cette section traitera de ceux qui ne décident *a priori* pas du contenu dommageable de l'information ou activité, ce que l'on appelle « *les intermédiaires techniques* ». Selon l'Office québécois de la langue française, l'expression « *intermédiaire* » se définit comme une « *personne ou organisme qui est chargé d'assurer la communication, la transmission des échanges d'idées ou de choses entre groupements ou individus du fait qu'il se trouve situé à un point de jonction ou de passage des uns aux autres* »[122]. À partir de cette définition, l'on peut affirmer que les « *intermédiaires techniques* » sont des personnes, entreprises ou organismes qui interviennent dans la chaîne de transmission de l'information circulant dans le réseau Internet à un point de jonction ou de passage des uns aux autres[123]. La caractéristique principale de ces acteurs est qu'ils ne contrôlent *a priori* pas l'information. Il faut préciser que l'on a volontairement choisi d'avoir recours à la terminologie se présentant dans la loi québécoise pour décrire les différents intermédiaires pour le simple motif que nous sommes situés sur le territoire québécois. Sont ainsi considérés comme des intermédiaires techniques, l'hébergeur, l'intermédiaire qui offre des services de conservation de documents technologiques, des services de référence à des documents

---

[122] Office québécois de la langue française, *Le grand dictionnaire terminologique*, Recherche –intermédiaire, en ligne sur : < http://www.granddictionnaire.com > (visité le 27 janvier 2009). Il s'agit de la définition se trouvant dans le domaine de la science de l'information.

[123] Celle retenue par le Professeur Trudel est la suivante : ce sont des « personnes, entreprises ou organismes qui interviennent dans l'accomplissement d'une tâche effectuée entre le point d'expédition d'une transmission de document et le point de réception final » : Pierre TRUDEL, « La responsabilité des acteurs du commerce électronique », *loc. cit.*, note 8, p. 616.

technologiques, le moteur de recherche, le fournisseur de services sur un réseau de communication[124].

Dans ce contexte, le mémoire définira les rôles joués par chacun, notamment celui de l'hébergeur.

A) L'hébergeur

L'hébergeur est un intermédiaire qui n'exerce *a priori* pas de contrôle sur l'activité litigieuse. La loi québécoise définit l'hébergeur comme celui *qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau de communication*[125]. La loi française énonce dans le même sens que l'hébergeur est *une personne physique ou morale qui met à la disposition du public des services de communication lui permettant de publier des contenus*[126]. La *Directive sur le commerce électronique* faisant écho à ces deux lois désigne une activité d'hébergement comme celle *consistant à stocker des informations fournies par un destinataire du service*[127]. Toutefois, la loi américaine[128] ne démontre pas une telle rigidité quant à la délimitation de cette notion, se contentant d'énoncer les concepts de l'utilisateur d'un service informatique interactif[129] et de fournisseur de contenus[130].

Les législateurs s'entendent ainsi pour dire que l'hébergeur est celui qui assure la conservation de fichiers, d'images et autres documents technologiques fournis par des utilisateurs de l'Internet dans des serveurs sur lesquels il détient un certain

---

[124] Pierre TRUDEL, « La responsabilité des acteurs du commerce électronique », *loc. cit.*, note 8, p. 616.

[125] L'article 22 de la *LCCJTI.*

[126] L'article 6.I.2 de la *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, *loc. cit.*, note 16 ; Pascal RENAUD, Thibault VERBIEST et Bertrand VANDEVELDE, « Le Web 2 dans l'entreprise: quelle responsabilité », 14 février 2008, en ligne sur : < http://www.droit-technologie.org/dossier-165/le-web-2-0-dans-l-entreprise-quelle-responsabilite.html > (visité le 19 janvier 2009).

[127] Directive *2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur* (ci-après citée « directive sur le commerce électronique »), *loc. cit*, note 15.

[128] L'article 230 de *Communications Decency Act*, *supra,* note 18, énonce ce qui suit : « *No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider* ». Cette loi sera abordée de façon plus détaillée dans le chapitre I du titre II de ce travail.

[129] Il est possible d'affirmer qu'un hébergeur est un utilisateur de service informatique interactif en lisant la definition suivante: « The term "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions »: 230(f)(2) ; voir également *Carafano* c. *Metrosplash.com Inc.*, 207 F. Supp. 2d 1055, 1065-66 (C.D. Cal. 2002).

[130] Le concept se définit comme suit: « The term "information content provider" means any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service »: *ibid.*

contrôle[131]. Si ce dernier a la possibilité de prendre connaissance de l'information qu'il héberge par le biais de ses installations, il est indubitable qu'il est de la même façon incapable de connaître le contenu de cette information et d'en apprécier le sens[132]. Il ne peut alors être assimilable à un fournisseur de contenus, compte tenu de la nature de son rôle qui s'éloigne de la fonction éditoriale.

Le rôle de l'hébergeur est comparable à celui du propriétaire des lieux[133]. Le fournisseur d'hébergement se voit confier des documents qui se trouvent sur la propriété de l'entreprise. Les propriétaires, tout comme l'hébergeur, ne peuvent être tenus responsables pour des actes posés par des tiers sur leur propriété lorsque les activités se déroulent à leur insu. La métaphore de propriétaire peut s'appliquer au prestataire d'hébergement: bien que l'information litigieuse se trouve sur la propriété de son serveur, il ne joue aucun rôle actif dans la diffusion de celle-ci[134]. À l'inverse, si le propriétaire ne fait rien pour retirer le contenu litigieux des murs de sa propriété alors qu'il a dûment été informé de ce fait, il sera alors considéré comme le rediffuseur de l'information, tout comme l'auteur du message[135]. Il en est de même pour l'hébergeur qui a de fait connaissance du déroulement de l'activité litigieuse. Par conséquent, il ressort de l'analogie avec le propriétaire des lieux que la connaissance du contenu litigieux est la condition préalable à l'imputation de responsabilité de l'hébergeur.

Les législateurs québécois, français, européen et américain s'entendent pour consacrer un régime d'exonération de responsabilité à l'hébergeur pour les contenus hébergés dans son serveur[136]. La limitation de responsabilité accordée à cet intermédiaire est toutefois conditionnelle à ce qu'il n'ait pas de fait connaissance de l'illicéité des activités se déroulant par le biais de ses services ou à ce qu'il retire le contenu litigieux ou assure la cessation de l'activité litigieuse dès qu'il est mis au courant du contenu illégal.

---

[131] Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit.*., note 47, p. 10.
[132] Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit.*., note 47, p. 10.
[133] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, « Droit du cyberespace », *op. cit.*, note 4, p. 5-10.
[134] Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit.*., note 47, p. 10.
[135] *ibid* ; *Hellar* c. *Bianco*, 11 Cal. App. 2d 424, 244 P.2d 757, 28 ALR2d 451 (1952) ; *Scott* c. *Hull*, 22 Ohio App.2d 141, 259 N.E.2d 160, (1970); *Tackett* c. *General Motors Corporation*, 836 F.2d 1042 (7th Cir. 1987); *Woodling* c. *Knickerbocker*, 17 N.W. 387 (Minn. 1883).
[136] Voir le chapitre I du titre II. En vertu de l'article 22 de la loi québécoise, l'article 6-I-2 de la loi française, l'article 14 de la *Directive sur le commerce électronique* et l'article 230 de la loi américaine.

L'analyse des législations mentionnées au paragraphe précédent porte à penser que la qualification d'hébergeur engage l'application d'un régime qui va limiter le régime de sa responsabilité[137]. Toutefois, il n'en est pas ainsi dans la jurisprudence actuelle. À cet égard, l'on assiste aujourd'hui à un contournement de cette règle par les tribunaux français qui n'hésitent pas à condamner les sites communautaires[138] malgré que le courant majoritaire français reconnaisse leur statut d'hébergeur[139]. À titre d'exemple, dans la décision *Monsieur Omar Sy et Monsieur Fred Testot et autres c. S.A. Dailymotion*[140], le TGI de Paris a estimé que le site *Dailymotion* se qualifiait d'hébergeur, soulignant que ce sont ses membres qui étaient les fournisseurs de contenus et a précisé que le fait de tirer un revenu substantiel du fait de la commercialisation d'espaces de publicité ne changeait en rien à ce raisonnement. La Cour a toutefois écarté l'exonération de responsabilité, jugeant que l'absence d'obligation légale de surveillance ne s'appliquait plus à partir du moment où les *activités sont induites ou générées par le prestataire lui-même*[141]. Le TGI de Paris a par conséquent conclu que ce site n'était plus considéré comme un hébergeur en ce qui concerne le contenu de l'information hébergée sur son réseau. De plus, dans la décision *Google* c. *Zadig productions*[142] qui fait écho à cette dernière, le TGI de Paris a condamné *Google* pour ne pas avoir retiré efficacement le contenu litigieux, bien qu'il en soit dûment informé. Le Tribunal reproche à l'hébergeur de ne pas avoir instauré un système technique empêchant la réapparition en ligne de la matière litigieuse. Il s'ensuit que le contenu illicite doit non seulement être enlevé mais aussi ne pas

---

[137] Pascal RENAUD, Thibault VERBIEST et Bertrand VANDEVELDE, « Le Web 2 dans l'entreprise: quelle responsabilité », *loc. cit.*, note 126. L'exonération de responsabilité est bien sûr conditionnelle à certains critères que les hébergeurs doivent remplir.

[138] *Monsieur Omar Sy et Monsieur Fred Testot et autres c. S.A. Dailymotion*, TGI Paris, 15 avril 2008 ; *Google* c. *Zadig productions*, TGI Paris, 19 octobre 2007, Juris-Data n°2007-344344, RDLI 2007/32 n°1062 obs. Costes L ; *ibid.*

[139] Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit.*, note 47, p. 15 ; Voir aussi *Groupe Mac. /Gilbert D*, TGI Lyon, 14e Ch., 21 juillet 2005, cité par B Tabaka, Commerce électronique : les plates-formes sont-telles des hénergeurs, RDLI2007/33n°1097, spéc. p. 12.

[140] *Précitée*, note 138; Pascal RENAUD, Thibault VERBIEST et Bertrand VANDEVELDE, « Le Web 2 dans l'entreprise: quelle responsabilité », *loc. cit.*, note 126, p. 7.

[141] *ibid.*

[142] *Précitée*, note 138 ; Pascal RENAUD, Thibault VERBIEST et Bertrand VANDEVELDE, *loc. cit.*, note 126. Dans cette décision, Google n'a retiré que de façon provisoire le contenu illicite puisque l'information était toujours disponible aux utilisateurs d'Internet après un premier retrait par Google.

réapparaître[143]. La jurisprudence française apporte ainsi une condition qui était jusque-là inexistante dans l'esprit de la loi[144].

L'analyse de la jurisprudence américaine illustre cette même ambiguïté quant à la délimitation des contours de la notion d'hébergeur. Dans la décision *Fair Housing Council of San Fernando Valley* c. *Roommate.com* [145], la Cour a établi que *Roommate* se qualifiait de fournisseur de contenus[146] puisqu'il posait des actes qui étaient de nature à créer ou structurer, partiellement ou totalement, le contenu de l'information fournie par ses membres[147]. Elle a ensuite conclu qu'il ne pouvait par conséquent se prévaloir de l'immunité prévue par la loi. Cette jurisprudence est toutefois contraire à la tendance jurisprudentielle américaine antérieure[148]. À cet égard, dans une décision dont les faits sont similaires[149], la Cour a jugé que *Matchmaker* ne pouvait se qualifier comme un fournisseur de contenus dès *lors qu'un profil ne contient aucun contenu jusqu'à ce qu'un utilisateur procède à son activation*. La Cour d'appel a souligné que « *le questionnaire [en question] facilitait l'indication des informations par les utilisateurs individuels [et] la sélection des réponses [était] laissée exclusivement à la discrétion de ces derniers* ». Par conséquent, la Cour a conclu que *« Matchmaker ne pouvait être tenu responsable, de l'association de certaines réponses à choix multiples avec un ensemble de caractéristiques physiques et une photographie ».*

En conclusion, le critère de contrôle effectif sur le contenu de l'information hébergée est généralement retenu par les tribunaux pour établir la distinction entre un

---

[143] *Google c/ Zadig productions*, *précitée*, note 142 ; Christophe CARON, « Contrefaçon et sites communautaires : état des lieux jurisprudentiel », Communication Commerce Électronique, n° 12, Décembre 2007, comm. 143.

[144] Pascal RENAUD, Thibault VERBIEST et Bertrand VANDEVELDE, *loc. cit.*, note 126.

[145] LLC, CV-03-09386-PA (9th Cir. May 15, 2007). Dans cette décision, l'opérateur du site Roommate.com qui se propose d'offrir à ses membres des services de colocation à l'aide d'outils techniques permettant la création de profils personnels a été poursuivi par avoir contrevenu aux lois relatives à la discrimination en matière de logement. La Cour a établi que pour se qualifier à ce titre, il ne devait jouer aucun rôle actif quant au contenu de l'information à être publiée par le biais de son serveur.

[146] La Cour s'exprime comme suit : « A content provider is « any person or entity that is responsible, *in whole or in part*, for the creation or development of information provided through the Internet." 47 U.S.C. § 230(f)(3).

[147] Si à l'inverse, l'opérateur du site Roommate.com, ne faisait que publier passivement l'information qu'il reçoit de ses membres, il serait alors considéré comme un simple fournisseur d'hébergement et serait visé par cette immunité : *Fair Housing Council of San Fernando Valley* c. *Roommate.com*, LLC, *précitée*, note 145. Voir également *Batzel* c. *Smith*, 333 F.3d 1018 (9th Cir. 2003).

[148] *Carafano* c. *Metrosplash.com Inc.*, *précitée*, note 129. Forum des droits sur l'Internet, « États-Unis: extension du régime de responsabilité allégée aux agences matrimoniales virtuelles », en ligne sur : < http://www.foruminternet.org/specialistes/veille-juridique/actualites/tats-unis-extension-du-regime-de-responsabilite-allegee-aux-agences-matrimoniales-virtuelles.html > (visité le 20 janvier 2009).

[149] *Carafano* c. *Metrosplash.com Inc.*, *précitée*, note 129. Dans cette décision, l'opérateur du site Matchmaker.com qui offre un service de rencontre matrimonial à ses membres est poursuivi sur la base d'atteinte à la vie privée. Les membres peuvent y créer leur propre profil à l'aide d'un questionnaire à choix multiples. Forum des droits sur l'Internet, « États-Unis: extension du régime de responsabilité allégée aux agences matrimoniales virtuelles », *loc. cit*, note 148.

responsable d'hébergement et un responsable de contenus[150]. Toutefois, l'on observe une certaine tendance des tribunaux à rechercher la responsabilité de l'hébergeur sur la base de critères qui ne se retrouvent nullement dans la loi[151]. L'on assiste alors à une tentative de reformulation de la notion d'hébergeur par les tribunaux, ce qui conduit à la rendre ambiguë au sein de la communauté juridique et incompréhensible par les intermédiaires.

Qu'en est-il de l'intermédiaire offrant des services de référence à des documents technologiques?

B) L'intermédiaire offrant des services de référence à des documents technologiques

L'intermédiaire ici visé est le prestataire qui agit à titre d'intermédiaire pour offrir des services de référence à des documents technologiques, à savoir un index, des hyperliens, des répertoires ou des outils de recherche[152]. Le Petit Robert définit le terme « *référence* » comme étant l'« *action de se référer ou de renvoyer le lecteur à un texte, une autorité* ». La notion d'intermédiaire offrant des services de référencement est définie dans la loi québécoise par le biais de l'article 22 de la LCCJTI. À l'inverse, la *Directive sur le commerce électronique* et la loi française demeurent silencieuses sur la délimitation de cette notion, ne prévoyant que des dispositions applicables à certains intermédiaires[153]. Il en est de même pour la loi américaine qui fournit des définitions larges aux concepts d'« utilisateur d'un service informatique interactif », de transmetteur et de fournisseur de contenus[154].

L'article 22 de la LCCJTI qui vise l'intermédiaire offrant des services de référencement à des documents technologiques énonce que ce dernier n'est pas responsable des activités commises par le biais de ses services. Il peut toutefois

---

[150] Notamment dans la jurisprudence américaine : *Doe* c. *MySpace*, *précitée*, note 105.

[151] *Monsieur Omar Sy et Monsieur Fred Testot et autres c. S.A. Dailymotion*, *précitée*, note 138 ; *Google* c. *Zadig productions*, *précitée*, note 138 ; *Fair Housing Council of San Fernando Valley* c. *Roommate.com*, LLC, *précitée*, note 145. Voir également *Batzel* c. *Smith*, 333 F.3d 1018 (9th Cir. 2003) ; Pascal RENAUD, Thibault VERBIEST et Bertrand VANDEVELDE, « Le Web 2 dans l'entreprise: quelle responsabilité », *loc. cit.*, note 126.

[152] Pierre TRUDEL, « La responsabilité des acteurs du commerce électronique », *loc. cit.*, note 8, p. 628.

[153] L'hébergeur, le transmetteur et l'intermédiaire qui conserve des documents à la seule fin d'assurer l'efficacité de la transmission sont énoncés aux articles 12 à 14 de la *Directive sur le commerce électronique* ainsi qu'aux articles 6-I-1 et 6.I-2 de la loi française. La jurisprudence française applique le statut d'hébergeur –ou d'éditeur, en quelques circonstances– à cet intermédiaire.

[154] Voir les articles 230(f)(1) et (4). L'intermédiaire en question peut être considéré comme un utilisateur d'un service informatique interactif au sens de la définition de l'article 230(f)(2) de *CDA*.

« *engager sa responsabilité s'il a de fait connaissance que les services qu'il fournit servent à la réalisation d'une activité illicite et s'il ne cesse pas promptement de fournir ses services aux personnes qu'il sait être engagées dans cette activité* »[155].

Le rôle de l'intermédiaire qui offre des services de référencement est comparable à celui du bibliothécaire[156]. Comme celui-ci, l'intermédiaire en question distribue de l'information contenue dans un système de référencement de données sur un support de stockage, dont un index, des hyperliens, des répertoires de recherche ou des outils de recherche. À l'instar du bibliothécaire, l'intermédiaire n'est pas responsable des activités se déroulant par le biais de ses services, étant donné qu'il ne maîtrise pas le contenu des informations qu'il transmet[157]. La responsabilité de cet intermédiaire ne sera déclenchée que s'il omet de retirer l'information dont il aura été informé du contenu litigieux[158].

La connaissance de l'illicéité des activités marque la ligne de départ de la responsabilité des intermédiaires prévus à l'article 22 de la loi québécoise. Or, l'on assiste aujourd'hui à l'émergence d'une multitude d'acteurs qui peuvent être considérés comme des intermédiaires dans la mesure où ils ne sont pas au courant de l'illicéité des activités se déroulant par le biais de leurs installations. À cet égard, l'on peut penser à un outil de recherche, au blogueur, à un opérateur de site de partage de contenus, à un opérateur de site de réseautage social et aux Wikis dont le statut d'intermédiaire ne sera plus applicable dès lors qu'ils maîtrisent le contenu de l'information litigieuse.

Les outils de recherche[159] sont des mécanismes fournissant un service d'indexation afin de retrouver les documents s'accordant à des critères de la requête que l'on effectue ou « *collection structurée et thématique de répertoires résultant d'une compilation d'un domaine d'information* ». Parmi les outils de recherche, l'on compte des moteurs de recherche et les annuaires ou répertoires de recherche.

---

[155] L'article 22 de la *LCCJTI*. Voir également le Titre II, du chapitre I, de la section II, du paragraphe III-B)-3.

[156] Pierre TRUDEL, « La responsabilité civile sur Internet selon la Loi concernant le cadre juridique des technologies de l'information », dans Service de la formation permanente, Barreau du Québec, *Développements récents en droit de l'Internet*, Cowansville, Éditions Yvon Blais, 2001, 119, en ligne sur : « http://www.crdp.umontreal.ca/cours/drt6929f/Resp.%20civile-int.fpbq11-01.pdf » (visité le 18 juin 2007).

[157] *ibid.*

[158] J. A GRAY, « Strict Liability for Dissemination of Dangerous Information? », (1990) 82 *Law Library Journal* 497.

[159] Pierre TRUDEL, « La responsabilité civile sur Internet selon la Loi concernant le cadre juridique des technologies de l'information » *loc. cit.*, note 156, p. 118.

Un moteur de recherche est un logiciel d'exploration ou un programme qui indexe automatiquement le contenu de différentes pages Web, notamment les sites Web, dans les bases de données, en fonction des mots-clés qu'elles contiennent, afin de permettre le repérage de l'information ainsi recherchée[160]. Lorsqu'une requête est lancée sur le site du moteur de recherche, le site Web ou le répertoire de recherche affiche une série de documents « hypertextualisés » qui sont classés selon un « score de pertinence » obtenu à partir de la fréquence d'occurrence de mots significatifs de la requête dans le document, leur proximité entre eux, leur présence dans le titre du document[161].

Le répertoire de recherche est un système de classification de données regroupant les données dans des catégories distinctes qui sont répertoriées sur un support de stockage, de manière à les rendre accessibles au public[162]. Un même répertoire peut renfermer plusieurs « sous-répertoires », ce qui permet de faciliter la consultation des données.

La loi québécoise pose le principe selon lequel cet intermédiaire ne peut être tenu responsable des activités accomplies au moyen de ses services que lorsqu'il acquiert connaissance du contenu illicite de l'activité en question ou dès qu'il omet de retirer le contenu litigieux[163]. Quant à la jurisprudence française, bien qu'elle applique généralement le statut d'hébergeur à cet intermédiaire[164], elle reprend en substance le même principe. À cet effet, le TGI de Paris a jugé que le moteur de recherche *Google* se qualifiait d'hébergeur, estimant qu'il permettait la mise à disposition de fichiers au public[165]. Le Tribunal a toutefois condamné *Google* pour ne pas avoir retiré de façon définitive le contenu illicite placé en ligne par des utilisateurs d'Internet alors qu'il en avait été dûment informé. La décision apporte une précision à ce principe : le contenu

---

[160] Thibault VERBIEST, « Commerce électronique : le nouveau cadre juridique : publicité, contrats, contentieux », Bruxelles, Éditions Larcier, 2004, p. 31.
[161] *ibid.*
[162] Pierre TRUDEL, « La responsabilité civile sur Internet selon la Loi concernant le cadre juridique des technologies de l'information », *loc. cit.*, note 156, p. 118.
[163] En vertu de l'alinéa 3 de l'article 22 de la *LCCJTI*.
[164] *Google c/ Zadig productions, précitée*, note 142 ; Pascal RENAUD, Thibault VERBIEST et Bertrand VANDEVELDE, « Le Web 2 dans l'entreprise: quelle responsabilité », *loc. cit.*, note 126, p. 7.
[165] *Google c/ Zadig productions, précitée*, note 142.

litigieux doit non seulement être retiré mais il doit aussi ne pas réapparaître car alors la connaissance du caractère illicite est acquise[166].

Les blogueurs sont les personnes qui tiennent un blogue, c'est-à-dire un site Web constitué d'une succession de billets ou d'articles classés suivant un ordre chronologique et enrichis d'hyperliens sur lesquels le lecteur est invité à apporter des commentaires[167]. Les billets ou articles peuvent renfermer des textes, des images ou des vidéos. Le blogueur a la faculté de *censurer* toutes informations dont le contenu lui *apparaît* comme étant illicite. Le blogue tient tout son intérêt de sa structure particulière : il s'agit non seulement d'un espace personnel à l'image d'un journal de bord appartenant au blogueur[168] mais relève également d'un espace public permettant aux utilisateurs d'Internet de s'exprimer. Ce double aspect du blogue soulève l'épineuse question de la qualification du maître de blogue[169]. Dans ce contexte, on peut se demander si ce dernier peut être considéré comme un hébergeur pour les messages qui sont diffusés par les tiers. Cette question ne semble pas définitivement réglée. Au Québec et aux États-Unis[170], l'on assimile le statut d'hébergeur au blogueur alors qu'en France, la doctrine demeure mitigée. À ce sujet, le Conseil Constitutionnel a précisé que la responsabilité d'un hébergeur ne peut être retenue, à moins que le caractère illicite de l'information dénoncée soit manifeste ou qu'un juge en ait ordonné le retrait[171]. Autrement dit, l'hébergeur dispose d'un pouvoir d'appréciation du contenu illicite des informations dénoncées par un tiers. C'est d'ailleurs

---

[166] *Google c/ Zadig productions*, *précitée*, note 142 ; Christophe CARON, « Contrefaçon et sites communautaires : état des lieux jurisprudentiel », *loc. cit.*, note 143.

[167] Office québécois de la langue française, *Le grand dictionnaire terminologique*, Recherche –blogue, en ligne sur : < http://www.granddictionnaire.com > (visité le 27 janvier 2009) ; Bernard BRUN, « Le blogue : un équilibre délicat entre communication et responsabilité », dans Leg@l.TI, 2007, Éd. Yvon Blais, p. 73, 75.

[168] Le blogue ressemble à un journal de bord : Office québécois de la langue française, *Le grand dictionnaire terminologique*, Recherche –blogue, en ligne sur : < http://www.granddictionnaire.com > (visité le 27 janvier 2009). Il s'agit de la définition se trouvant dans le domaine de l'informatique ; TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit.*, note 47, p. 13.

[169] À cet égard, Lionel Thoumyre affirme que « *l'internaute responsable d'un blogue sera, a priori, considéré comme un éditeur de service de communication en ligne s'agissant des contenus qu'il publie lui-même volontairement et comme un organisateur de forums pour les fils de discussion figurant à la suite des articles* » : Lionel THOUMYRE, « La responsabilité pénale et extracontractuelle des acteurs de l'Internet », Lamy, droit des médias et de la communication, juin 2007, étude 464.

[170] Les articles 22(3) de la *LCCJTI* et 230 de *CDA* accordent une immunité à celui-ci, à condition de respecter certaines exigences.

[171] La définition d'hébergeur telle que prévue à l'article 6.I.2 de la *LCEN* étant très large, on peut l'appliquer au maître de blogue. Le Conseil Constitutionnel s'est prononcé sur la validité des dispositions régissant les obligations mises à la charge de ce prestataire : il a déclaré que les articles 6.I.2 et 6.I.3 de la *LCEN* « *ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge* » : *Décision du Conseil Constitutionnel* du 10 juin 2004, n°2004-496.

l'interprétation qui a été retenue par une décision de la Cour d'appel de Paris qui a condamné *Google* en tant qu'hébergeur[172].

Les sites de partage de contenus sont des sites Web qui permettent aux utilisateurs de mettre en ligne des fichiers, comme des vidéos, des images ou des livres, afin de partager leurs contenus. À titre d'exemple, l'on retrouve *Youtube* ou *Dailymotion*[173]. Ces sites sont assimilables à l'hébergeur en ce qui concerne les fichiers déposés par les tiers. Toutefois, l'on observe une tendance à également tenir compte du rôle prépondérant du maître de site dans la structure de présentation de celui-ci pour fonder la responsabilité du maître du site[174].

Les sites de réseautage social offrent aux personnes un service de rencontre ou de mise en relation par le biais de leurs réseaux sociaux[175]. La jurisprudence considère qu'à l'égard des contenus déposés par les usagers du site, le maître du site est généralement dans une position d'hébergeur[176]. Il y a cependant un courant jurisprudentiel qui prend également en considération le degré d'implication résultant de la configuration du site Web[177]. À cet égard, dans l'affaire *Lafesse*[178], le TGI de Paris a qualifié le maître du site de réseautage social d'éditeur sur la base de ce critère.

Le wiki est un site Web qui permet aux usagers de modifier l'information s'y trouvant[179]. À l'image d'une plateforme de travail collectif, ce site a des finalités d'information au public[180]. Les usagers peuvent, à leur guise, corriger l'information qu'ils jugent inexacte ou incomplète. Par contre, les Wikis peuvent aussi contenir des règles relatives à l'utilisation du site, notamment sur les propos litigieux ou sur les paramètres de modification du site. À l'instar du blogue, les fonctionnalités des sites

---

[172] *Google Inc.* c./ *Benetton*, Bencom, Cour d'appel de Paris, 14 ième chambre, section A, Arrêt du 12 décembre 2007, en ligne sur : < http://www.legalis.net/jurisprudence-decision.php3?id_article=2116 > (visité le 26 janvier 2009) ; *Google*, condamné en tant qu'hébergeur de blog, Légalis.net, 17 décembre 2007, en ligne sur : < http://www.legalis.net/breves-article.php3?id_article=2117 > (visité le 26 janvier 2009). Toutefois, le droit substantif français ne reconnaît toujours pas une telle interprétation.

[173] Aussi connus sous le nom de *Social Networking Services* : Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit.*, note 47, p. 14.

[174] *Monsieur Omar Sy et Monsieur Fred Testot et autres c. S.A. Dailymotion*, *précitée*, note 138 ; *Google* c. *Zadig productions*, *précitée*, note 138 ; *Fair Housing Council of San Fernando Valley* c. *Roommate.com*, LLC, *précitée*, note 145 ; Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit..*, note 47, p. 14.

[175]: *ibid.* À titre d'exemple, il y a le site MySpace.

[176] Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit..*, note 47, p. 15.

[177] Jean-Yves L. dit *LAFESSE / Myspace*, *précitée*, note 105 ; *ibid*, p. 15.

[178] Jean-Yves L. dit *LAFESSE / Myspace*, *précitée*, note 105.

[179] L'encyclopédie en ligne Wikipédia en constitue un bon exemple : *ibid*; Office québécois de la langue française, *Le grand dictionnaire terminologique*, Recherche –wiki, en ligne sur : < http://www.granddictionnaire.com > (visité le 27 janvier 2009).

[180] Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit..*, note 47, p. 18.

Wikis présentent donc une situation où les statuts d'hébergement et d'éditeur s'entrechoquent plus que jamais. La jurisprudence majoritaire assimile les sites Wikis au statut d'hébergeur pour les informations provenant des tiers[181]. À cet égard, dans une ordonnance de référé du 29 octobre 2007, le TGI de Paris a écarté la responsabilité de l'encyclopédie en ligne *Wikipédia* en ce qui concerne le contenu des articles publiés, estimant qu'elle se qualifiait d'hébergeur[182]. Dans cette affaire, les demandeurs n'avaient pas respecté les règles procédurales prévues dans la *LCEN* visant la notification de l'information litigieuse. De ce fait, *Wikipédia* n'était pas réputé avoir connaissance de l'illicéité des informations figurant dans l'article et n'était donc pas tenu de supprimer les passages contestés[183].

En conclusion, il y a lieu d'observer que le concept d'intermédiaire offrant des services de référence à des documents technologiques se rapporte généralement au statut de l'hébergeur mais il existe tout de même une certaine tendance jurisprudentielle qui assimile cet intermédiaire au statut d'éditeur[184].

Examinons maintenant l'intermédiaire qui conserve les documents à la seule fin d'assurer l'efficacité de leur transmission ultérieure.

C) L'intermédiaire qui conserve les documents à la seule fin d'assurer l'efficacité de leur transmission ultérieure

L'intermédiaire qui est visé ici est l'intermédiaire qui conserve sur un réseau de communication les documents technologiques à la seule fin d'assurer l'efficacité de leur transmission ultérieure. Il s'agit d'un serveur à accès contrôlé, d'un hébergeur pour des documents destinés à des personnes spécifiquement désignées ou bien encore

---

[181] *Marianne B. et autres/ Wikimedia Foundation*, Tribunal de grande instance de Paris, Ordonnance de référé 29 octobre 2007, en ligne sur : < http://www.legalis.net/jurisprudence-decision.php3?id_article=2071>, (visité le 28 janvier 2009) ; *ibid.*

[182] *ibid* ; Le site collaboratif avait été assigné par trois personnes en raison du contenu d'un article révélant leur orientation sexuelle.

[183] Certains pensent qu'il faut relativiser cette décision pour les motifs suivants : i) il s'agit d'une ordonnance de référé qui ne juge que de l'évidence ; ii) une absence de dommages directs en raison de la suppression de l'article litigieux; iii) les parties ont convenu d'assigner *Wikipédia* en tant qu'hébergeur alors que ce statut ne va pas de soi : « Wikipédia, hébergeur sans obligation », *legalis.net*, 8 novembre 2007, en ligne sur : < http://www.legalis.net/article.php3?id_article=2073 > (visité le 28 janvier 2009) ; Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit.*, note 47, p. 19.

[184] Jean-Yves L. dit *LAFESSE / Myspace*, *précitée*, note 105 ; *Monsieur Omar Sy et Monsieur Fred Testot et autres c. S.A. Dailymotion*, *précitée*, note 138 ; *Google* c. *Zadig productions*, *précitée*, note 138 ; *Fair Housing Council of San Fernando Valley* c. *Roommate.com*, LLC, *précitée*, note 145 ; Julien TAÏEB, « Prestataires techniques de l'Internet : le sens des responsabilités », *loc. cit*, note 105.

d'un prestataire offrant un service d'intranet[185]. À l'instar de la loi française[186], la loi québécoise[187] et la *Directive sur le commerce électronique* visent directement l'intermédiaire qui conserve les documents technologiques pour rendre plus efficace leur transmission ultérieure alors que la loi américaine ne traite pas de manière spécifique la responsabilité imputable à ce dernier[188]. Contrairement à la loi québécoise, les lois américaine et française ainsi que la *Directive sur le commerce électronique* comportent des dispositions également applicables sur le plan pénal[189]. Les législateurs européen, français, américain et québécois s'entendent toutefois pour organiser un régime d'exonération de responsabilité applicable à celui-ci. En principe, cet intermédiaire ne répond pas des activités accomplies par des tiers au moyen de documents conservés par ce dernier ; son rôle est assimilable à celui du transmetteur[190].

L'intermédiaire dont on parle ici est celui qui se voit confier des documents par des tiers et conserve ceux-ci dans l'unique but d'en assurer l'efficacité de la transmission. Cette fonction peut être réalisée par différentes façons. Elle peut se faire par l'antémémorisation ou le *caching* qui est un procédé permettant le stockage des éléments d'une page Web dans un serveur ou un ordinateur, de manière à accéder plus efficacement à la page Web « *sans qu'il soit nécessaire de requérir le document au serveur sur lequel il est originellement situé* »[191]. L'antémémorisation peut être pratiquée autant par les exploitants des réseaux, par les usagers que par des proxies qui sont des intermédiaires entre le navigateur de l'usager et le serveur Web[192]. Les proxies servent à la fois de filtres et de caches. En effet, plusieurs exploitants de réseaux font passer leurs clients par un proxy avant de les diriger sur le réseau Internet[193]. Les auteurs Michael Tischer et Bruno Jennrich déclarent que : « *[l]a caractéristique principale d'un*

---

[185] Pierre TRUDEL, « La responsabilité des acteurs du commerce électronique », *loc. cit.*, note 8, p. 642.
[186] En vertu de l'article 9 de la *LCEN* qui modifie l'article L32-3-4 du *Code des postes et des communications électroniques*.
[187] En vertu des articles 37 de la *LCCJTI* et 13 de la *Directive sur le commerce électronique*.
[188] Le régime de responsabilité applicable à cet intermédiaire découle de l'interprétation de l'article 230(f)(4) de *Communications Decency Act* qui traite de la responsabilité du transmetteur.
[189] Voir l'article 13 de la *Directive sur le commerce électronique* et l'article 9 de la *LCEN* et 230 de la *CDA*
[190] Le régime de responsabilité imputable à cet intermédiaire sera discuté dans le Titre II, du chapitre I, de la section II, du paragraphe III-C)-1.
[191] *ibid.*, p. 643.
[192] *ibid.*, p. 643.
[193] Michael TISCHER et Bruno JENNRICH, « La bible Internet expertise et programmation », Paris, Micro Application, 1997, p. 1050.

proxy est sa fonction de point de passage obligé par les accès Web des hôtes reliés. Si l'un des ordinateurs lance son navigateur pour accéder au réseau et à l'un des serveurs disponibles, la requête passe d'abord par le proxy. C'est lui qui prend le contrôle des opérations, reprend la requête en son propre nom pour le transmettre au serveur concerné. Lorsque les informations réclamées arrivent, le proxy les renvoie à l'hôte du demandeur, qui ignore sa démarche. En fait, le proxy se comportant comme le serveur, l'hôte ne perçoit pas son existence »[194].

L'antémémorisation présente une particularité intéressante de réduire le délai d'attente lors de l'accès aux sites Web par les clients. Ce délai peut survenir lorsque les internautes désirent accéder à des sites Web éloignés. Pour contrer cet inconvénient, les exploitants de réseau procèdent à l'antémémorisation des sites éloignés en stockant les documents les plus fréquemment consultés sur le proxy, ce qui rendra plus rapide l'accès aux sites web par les clients[195].

Les législations précitées (européennes, française et américaine) établissent un régime d'exonération de responsabilité à l'égard de l'intermédiaire qui conserve des documents technologiques à la seule fin d'assurer l'efficacité de leur transmission ultérieure. Toutefois, à l'exception de la loi américaine[196], ces législations énumèrent les situations dans lesquelles la responsabilité de cet intermédiaire peut être engagée. Il peut ainsi être tenu responsable de l'information litigieuse en modifiant l'information du document[197] ou en ne respectant pas les conditions d'accès au document[198] ou en entravant le cours de l'utilisation licite et usuelle de la technologie utilisée pour obtenir des données sur l'utilisation de l'information[199]. Par ailleurs, la responsabilité de cet intermédiaire peut être également engagée s'il ne retire pas promptement du réseau ou s'il ne rend pas l'accès au document impossible alors qu'il a de fait connaissance qu'un tel document a été retiré de là où il se trouvait initialement sur le réseau, du fait qu'il

---

[194] *ibid*, p. 1050.
[195] *ibid.*, p. 644.
[196] La loi américaine n'énonce que le concept général, en précisant que le prestataire est exonéré tant qu'il ne se qualifie pas de fournisseur de contenus : art. 230(c)(2) de *CDA*.
[197] Sur ce point, la loi québécoise se montre plus explicite en énonçant toutes les situations qui correspondent à une participation à l'action d'autrui. L'on retrouve ainsi à l'article 36 de la *LCCJTI* les cas de figure suivants : être à l'origine de la transmission du document ; sélectionner ou modifier l'information du document ; sélectionner la personne qui transmet le document, qui le reçoit ou qui y a accès ou conserver le document plus longtemps que nécessaire pour sa transmission. Voir les articles 37 de la *LCCJTI*, 13 de la *Directive sur le commerce électronique* et 9 de la *LCEN*.
[198] La *Directive sur le commerce électronique* à son article 13 et la loi française à son article 9 énoncent également le cas où le prestataire ne se conforme pas aux règles concernant la mise à jour de l'information.
[199] Dans ce cas de figure, la loi québécoise emploie une terminologie différente dans son article 37 qui précise que la responsabilité de cet intermédiaire peut être engagée « en prenant des mesures pour empêcher la vérification de qui a eu accès au document ».

n'est pas possible aux personnes qui y ont droit d'y avoir accès ou du fait qu'une autorité compétente en a ordonné le retrait du réseau ou en a interdit l'accès[200]. Si l'intermédiaire se retrouve dans l'une ou l'autre de ces situations, il ne peut plus être qualifié de simple transmetteur. En posant l'un ou l'autre de ces gestes, il se retrouve à prendre une part active dans la décision de diffuser le document : son rôle de simple transmetteur ne tient plus, il devient alors un éditeur.

Après avoir examiné cette notion, analysons maintenant au concept de transmetteur.

D) Le transmetteur

Le transmetteur est le prestataire de services qui n'intervient que pour la transmission de l'information sur un réseau de communication. Le rôle de ce dernier est de transporter de l'information d'un site à un autre. Il est également connu sous l'appellation « *common carriers* » ou de « *fournisseur de services Internet* ». La notion de transmetteur est explicitement définie dans les lois québécoise, française et américaine ainsi que dans la *Directive sur le commerce électronique* [201]. Malgré de légères nuances dans la définition de cette notion[202], les législateurs s'entendent pour accorder à ce prestataire le rôle de transporteur, c'est-à-dire celui qui n'intervient sur le réseau que pour l'acheminement de l'information. À titre d'exemple, un utilisateur d'Internet qui souhaite accéder à son courriel fait appel au service de son fournisseur de service. L'utilisateur en question expédie le courriel au moyen du serveur de courriel. Le message envoyé est conservé dans une base de données du courriel et archivé au nom de l'usager[203]. Ce prestataire n'agit que lors de la transmission du courriel vers le destinataire.

---

[200] En vertu des articles 37 de la *LCCJTI*, 13 de la *Directive sur le commerce électronique* et 9 de la *LCEN*.

[201] Les articles 36 de la *LCCJTI*, 6-I-1 de la *LCEN* et 9 de la *LCEN* (ce dernier article introduit le L. 32-3-4 du *Code des postes et des communications électroniques*), 230(f)(4) de *CDA* et l'article 12 de la *Directive sur le commerce électronique*.

[202] La loi québécoise et la *Directive sur le commerce électronique* font référence à une fourniture de service sur un réseau de communication pour la transmission de l'information alors que la loi française, reprenant la formulation que l'on retrouve dans ces deux textes de lois, précise qu'il s'agit de toute personne qui assure une activité de transmission de contenus sur un réseau de communications électroniques ou fourniture d'accès à un réseau de communication : *ibid.*

[203] Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit..*, note 47, p. 26.

En règle générale, le transmetteur est exonéré de sa responsabilité, à condition d'assumer un rôle passif pour l'acheminement de l'information[204]. N'agissant que comme un simple transmetteur, ce dernier n'est pas tenu responsable des actions accomplies par autrui au moyen des documents qu'il transmet pour ses clients et pendant la durée nécessaire pour en assurer l'efficacité[205]. Toutefois, les législateurs québécois, français et européen prévoient des situations dans lesquelles sa responsabilité peut être engagée, à savoir être à l'origine de la transmission, sélectionner le destinataire de la transmission et sélectionner ou modifier les informations contenues dans le document[206]. Contrairement aux législateurs français et européen, le législateur québécois prévoit un autre cas de figure, à savoir la conservation du document plus longtemps que nécessaire pour sa transmission. Les quatre cas de figure mentionnés[207] correspondent à une situation où le prestataire se retrouve à jouer un rôle actif dans la transmission de l'information. De ce fait, il ne peut plus se qualifier de simple transmetteur.

Dans cette section, l'on a décrit chacun des intermédiaires techniques faisant l'objet du mémoire, à savoir l'hébergeur, l'intermédiaire offrant des services de référence à des documents technologiques, l'intermédiaire qui conserve des documents à la seule fin d'assurer l'efficacité de leur transmission ultérieure et le transmetteur. L'on a examiné les définitions fournies par les lois québécoise, française, américaine ainsi que la *Directive sur le commerce électronique*. L'on a dégagé les similitudes et distinctions entre chacune de ces lois ainsi que les tendances jurisprudentielles s'y reliant.

À la lumière de cette analyse, il y a lieu de constater que le concept d'intermédiaire technique n'est pas une notion figée, elle peut changer très rapidement et être sujette à une série d'obligations qui s'établissent en fonction du rôle joué par chacun d'eux. Or, l'on assiste aujourd'hui à une augmentation du nombre d'intermédiaires. Devant ce fait, la circonscription des contours de chacun des

---

[204] Les articles 36 de la *LCCJTI*, 6-I-1 de *la LCEN* et 9 de la *LCEN* (ce dernier article introduit le L. 32-3-4 du *Code des postes et des communications électroniques*), 230(c)(2) de *CDA* et l'article 12 de la *Directive sur le commerce électronique*.

[205] En vertu de l'article 36 de la *LCCJTI*.

[206] *Supra*, note 186. Le législateur ne fait qu'énoncer le principe général selon lequel le transmetteur, pour bénéficier de l'exonération de responsabilité, ne doit exercer aucun contrôle sur le contenu de l'information.

[207] Cette liste n'étant pas exhaustive, il y a d'autres situations qui peuvent donner ouverture à la responsabilité du transmetteur : Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit.*., note 47, p. 26.

concepts devient difficile : d'où la présence d'ailleurs de contradictions dans la jurisprudence de différents pays. En outre, il faut comprendre que l'intermédiaire n'assume pas de responsabilité du fait de l'accomplissement d'activités illicites au moyen de ses services, pour autant qu'il agisse effectivement comme tel.

Après avoir défini en quoi consiste la notion d'intermédiaires techniques, l'on analysera, à la lumière de législations de différents pays, les mécanismes qui permettent d'évaluer la responsabilité de ces intermédiaires.

TITRE II- LA RESPONSABILITÉ DES INTERMÉDIAIRES TECHNIQUES À LA LUMIÈRE DES PRATIQUES INTERNATIONALES EN COMPARAISON AVEC LE DROIT PÉNAL CANADIEN

Dans le deuxième titre, il y a lieu d'analyser, en premier lieu, les normes et pratiques internationales qui régissent la responsabilité pénale des intermédiaires techniques. Cette analyse permettra de situer et d'évaluer le régime de responsabilité imputable à ces intermédiaires. Plus précisément, ce titre fera l'analyse des principes qui se déduisent des normes internationales en ce qui concerne l'imputation de responsabilité des intermédiaires techniques, à savoir les principes de contrôle, de connaissance et de l'absence d'obligation légale de surveillance. L'on a volontairement choisi de recourir à ces principes pour évaluer le régime de responsabilité applicable aux intermédiaires techniques, en posant que ces principes sont à la base de l'imputation de leur responsabilité pénale. Toutefois, il faut se garder de voir là des principes impératifs à partir desquels découlent des obligations que tous les intermédiaires techniques doivent respecter.

Cette mise en garde étant faite, l'on pourra alors amorcer l'étude des différents principes qui se déduisent des normes et pratiques internationales et se situant à la base de l'imputation de responsabilité des intermédiaires techniques.

CHAPITRE I- Les principes régissant l'imputation d'une responsabilité à des intermédiaires techniques

Dans le premier chapitre, il y a lieu d'introduire les principes qui sont à la base de l'imputation de responsabilité des intermédiaires techniques. Puisque, afin de bien situer les rôles et responsabilités de chacun d'eux, il est essentiel d'identifier

adéquatement les principaux facteurs qui engagent leur responsabilité pour ensuite en dégager des « *principes d'imputabilité* » applicables à ces derniers.

Dans cette perspective, il y a lieu de faire l'étude des principes de contrôle, de connaissance et de l'absence d'obligation légale de surveillance tout au long du premier chapitre. Ces trois principes constituent la pierre angulaire de la responsabilité pénale des intermédiaires techniques dans le contexte d'Internet, en plus de s'imprégner dans les textes nationaux et internationaux comme des principes fondamentaux de la responsabilité pénale des intermédiaires techniques. Les trois principes seront alors examinés dans les trois premières sections de ce chapitre par le biais d'une étude législative et jurisprudentielle pertinentes. L'on pourra ainsi dégager les ressemblances et différences entre ces législations pour chacun des principes.

Section I- Le contrôle de l'information

Dans la première section de ce chapitre, il convient d'étudier le principe de contrôle de l'information en tant que premier principe d'imputation de responsabilité. La possibilité d'imputer une responsabilité à un acteur d'Internet suppose que l'on puisse identifier ceux qui ont la maîtrise de l'information dans divers réseaux de l'environnement électronique[208]. Le critère de contrôle est un élément constitutif de faute qu'il faut démontrer afin d'imputer une responsabilité à un acteur d'Internet. À cet effet, l'auteur Henry H. Perritt Jr. explique que : « *[p]our ces trois catégories de responsabilité juridique (diffamation, infraction au droit d'auteur et atteinte à la vie privée), on ne peut prouver l'existence de la faute sans montrer que l'acteur et auteur présumé de la faute a soit exercé un contrôle effectif sur le contenu de l'information, soit qu'il lui était possible de contrôler le contenu et de prévoir l'éventualité d'un préjudice s'il n'exerçait pas ce contrôle* »[209].

Afin d'imputer une responsabilité aux différents intermédiaires techniques, encore faut-il examiner la relation qu'ils ont avec le contenu du message transmis[210].

---

[208] Pierre TRUDEL et R. GÉRIN-LAJOIE, « La protection des droits et des valeurs dans la gestion des réseaux ouverts », *op.cit*, note 91, p. 324-325.

[209] Henry H. PERRITT Jr., « Tort liability, the first amendment and equal access to electronic networks », (1992) 5 *Harvard Journal of Law & Technology*, 65, 110-111.

[210] J.R. McDANIEL, « Electronic Torts and Videotext-At the Junction of Commerce and Communications », (1992) 18 *Rutgers Computer & Technology Law Journal*, 773 et 823.

La possibilité d'imputer une responsabilité à un intervenant dans la communication électronique dépend du degré de contrôle et de maîtrise qu'il exerce ou qu'il est réputé exercer sur le contenu de l'information circulant dans les réseaux ouverts. À cet égard, l'auteur Éric Schlachter déclare que : « *[i]l existe une échelle mobile du contrôle de l'information en ce qui concerne l'accès obligatoire. D'un côté, il y a les éditeurs primaires qui exercent un pouvoir discrétionnaire virtuellement presque illimité sur ce qu'ils impriment ou sur ceux à qui ils donnent accès ou diffusent l'information. On trouve aussi des titulaires des droits de propriété privée qui sont de la même façon protégés de l'accès obligatoire. À l'autre bout de cette échelle mobile, on trouve les opérateurs de communication qui, par définition, doivent être à la disposition de tous les utilisateurs et ne peuvent refuser de façon discriminatoire de fournir les services* »[211].

L'échelle mobile permet de refléter le fait que la notion de contrôle n'est pas figée : elle peut varier selon l'intensité de contrôle exercée par chacun sur l'activité en question. C'est à partir de cette intensité de contrôle que l'on peut d'ailleurs arriver à mieux définir les rôles de chacun d'eux. À cet égard, il faut observer que le contrôle peut prendre deux formes : un contrôle physique ou un contrôle du sens.

a) Le contrôle physique

Le contrôle physique suppose pour l'intermédiaire de pouvoir retirer l'information ou d'en empêcher l'accès afin de faire cesser la commission de toute activité illicite. Le contrôle physique est donc l'un des facteurs d'imputabilité permettant de fixer les paramètres entourant la responsabilité de ces derniers.

Quant à la question de savoir le moment où doit s'effectuer le contrôle physique, il faut examiner la durée pendant laquelle l'intermédiaire pouvait raisonnablement exercer un tel contrôle. Si, en raison de la courte durée de l'activité, il ne pouvait raisonnablement ou possiblement pas faire cesser l'activité en question avant qu'un tiers subisse un dommage, il serait difficile de voir au nom de quoi on pourrait lui imputer une responsabilité, étant donné la courte durée d'intervention qu'il avait sur cette activité. À l'inverse, si la durée d'intervention est beaucoup plus longue et que l'activité dure plus longtemps, l'intermédiaire en question aura plus de temps

[211] Éric SCHLACHTER, « Cyberspace, the free market and the free marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions », *supra*, note 19, p. 113. Il s'agit de notre traduction.

pour réagir et prendre des mesures pour empêcher la poursuite de cette activité. Dans cette hypothèse, on lui imputera une responsabilité plus lourde car l'on suppose qu'il avait assez de temps pour agir de façon diligente et prudente.

À cet effet, l'auteur Henry H. Perritt Jr. mentionne que la possibilité de déterminer le contrôle physique de l'information revêt également une dimension économique : « *[l]a victime préférerait une disposition qui permettrait à la personne incriminée de décliner sa responsabilité juridique seulement dans les cas où le contrôle du contenu de l'information est technologiquement impossible. Toutefois, la notion d'impossibilité revêt ici une dimension économique. La détermination de ce qui est possible exige de comparer les risques et les avantages* »[212].

Il faut donc se demander si l'intermédiaire en question pouvait effectivement agir sur l'activité illicite afin de la prévenir ou la limiter.

b) Le contrôle du sens

Le contrôle du sens implique la faculté pour l'intermédiaire d'exercer un pouvoir d'intervention sur le contenu de l'information. Contrôler le sens de l'information signifie la possibilité pour l'auteur de modifier, altérer, détruire ou retirer le contenu de l'information. Celui qui exerce un contrôle effectif sur le contenu de l'information a la possibilité de mettre fin à sa circulation en retirant matériellement une partie ou l'ensemble de l'œuvre. L'intermédiaire qui contrôle le contenu de l'information doit certainement répondre du dommage qui résulte de son caractère illicite. C'est pourquoi le contrôle du sens doit être compris comme un facteur d'imputabilité régissant la responsabilité des intermédiaires techniques.

Les commentaires formulés précédemment au sujet du moment à partir duquel le contrôle physique doit s'effectuer s'appliquent également pour le contrôle du sens. Si, en raison de la courte durée de l'information, l'intermédiaire ne pouvait raisonnablement pas vérifier son exactitude, et en conséquence, retirer le contenu dommageable, il peut être difficile de lui imputer une responsabilité. Si, au contraire, l'information transige pendant un laps de temps plus long, l'intermédiaire aura certainement le temps d'agir pour enlever ce qui est dommageable. Ainsi, dans le cas

---

[212] Henry H. PERRITT JR., « Tort liability, the first amendment and equal access to electronic networks », *loc. cit.*, note 209, p. 110-111.

de ceux qui interviennent dans la transmission de l'information, il convient de se demander, lorsqu'un événement dommageable survient, si l'intermédiaire en question pouvait raisonnablement agir de façon effective sur le contenu de l'information afin de prévenir ou limiter le dommage.

En résumé, le principe de contrôle apparaît comme un pré-requis à l'imputation de responsabilité car l'intervenant de la communication électronique doit pouvoir exercer un certain contrôle sur le contenu de l'information pour voir sa responsabilité engagée. Cette section fera l'étude du principe de contrôle en tant que l'un des principes fondamentaux d'imputation de responsabilité à partir des différentes interprétations qui ont donné lieu ce principe dans plusieurs lois et conventions, à savoir la *Convention sur la cybercriminalité*, la *Directive sur le commerce électronique*, la *Loi pour la confiance dans l'économie numérique*, la *Loi concernant le cadre juridique des technologies de l'information* et le *Communications Decency Act*.

A) La *Convention sur la cybercriminalité*

Dans cette section, il convient d'étudier la *Convention sur la cybercriminalité* et le Protocole afin de voir comment s'articule la notion de contrôle à l'égard des intermédiaires techniques.

Premièrement, commençons tout d'abord par la Convention. Cet instrument international prévoit des dispositions[213] qui supposent l'exercice d'un contrôle visant uniquement l'auteur du crime, c'est-à-dire celui qui est à l'origine de la commission de l'infraction[214]. Seule la disposition qui traite de la complicité[215] se trouve directement applicable aux intermédiaires techniques. Toutefois, cette disposition ne fait pas de distinctions entre chacun des intermédiaires puisqu'elle s'applique uniformément à l'égard de tous. Il est à préciser que la disposition qui traite de la complicité ne se

---

[213] Les articles 2 à 10 érigent en infractions pénales différents types d'activités pouvant être commis dans l'environnement Internet : *Convention sur la cybercriminalité*, Rapport explicatif, *loc. cit.*, note 24, par. 11.

[214] Voir les articles 2 à 10 de la Convention. Ces dispositions se retrouvent dans la Section I du Chapitre II qui est alloué aux infractions de la Convention.

[215] En vertu de l'article 11 de la Convention, dans la mesure où les intermédiaires techniques agissent comme tels. Cette disposition renvoie aux infractions établies en vertu des articles 2 à 10 de la Convention. L'infraction de tentative de commettre les infractions définies par la Convention est également prévue à l'article 11 de la Convention.

présente pas dans les autres législations nationales et internationales[216] qui sont plutôt un outil de sanction civile –avec l'ajout, selon le cas, de mécanismes de droit pénal et de procédure pénale[217] alors que ce texte international constitue tout d'abord un instrument de répression pénale.

Aux termes du premier paragraphe de la disposition sanctionnant la complicité[218], la responsabilité de l'intermédiaire technique peut être engagée lorsque ce dernier apporte une aide à l'auteur du crime avec l'intention[219] que l'une des infractions listées dans la Convention[220] soit commise. Comme le précise le rapport explicatif, pour que la responsabilité de l'intermédiaire puisse être engagée en vertu de cette disposition, il ne suffit pas que l'intermédiaire exerce un certain contrôle sur l'activité illicite : il doit de plus avoir connaissance du caractère illicite de cette activité et avoir l'intention qu'une telle infraction soit commise[221]. À cet égard, l'on retrouve plusieurs exemples de situations qui peuvent illustrer la nécessité de retrouver de façon cumulative les critères de connaissance et de contrôle comme éléments constitutifs d'une infraction. À titre d'exemple, prenons le cas où l'intermédiaire accomplit des actes en vue d'aider l'auteur du crime à accéder illégalement dans un système informatique[222] et à porter atteinte à l'intégrité des données[223] et du système[224]. Ainsi,

---

[216] C'est-à-dire la *Directive sur le commerce électronique*, la *Loi pour la confiance dans l'économie numérique* et le *Communications Decency Act*.

[217] C'est le cas pour la *Directive sur le commerce électronique* dans ses 12 à 15 et la *Loi pour la confiance dans l'économie numérique*, dans ses articles 6 et 9.

[218] Le premier paragraphe de l'article 11 de la Convention dispose que : « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise ».

[219] De plus, en vertu de ce paragraphe, l'intermédiaire doit non seulement avoir l'intention d'aider l'auteur du crime dans la commission du crime mais il doit également avoir l'intention que l'une des infractions soit perpétrée par cet auteur : *Convention sur la cybercriminalité*, Rapport explicatif, *loc. cit.*, note 24, par. 119 et 121 ; voir également l'article 11 de la Convention.

[220] *Convention sur la cybercriminalité*, Rapport explicatif, *loc. cit.*, note 24, par. 119.

[221] Le rapport explicatif énonce ce qui suit : « [a]insi, par exemple, bien que la transmission par le biais de l'Internet de données relatives à un contenu nuisible ou d'un code malveillant requiert l'assistance de fournisseurs de services agissant comme intermédiaires, un fournisseur de services qui n'a pas d'intention criminelle ne peut être tenu responsable au titre de cette section » : *Convention sur la cybercriminalité*, Rapport explicatif, *loc. cit.*, note 24, par. 119. Voir également le paragraphe 105 du rapport explicatif qui rapporte ce qui suit : « [a]insi, par exemple, la responsabilité peut être imposée s'il y a "connaissance et contrôle" de l'information transmise ou stockée. Il ne suffit pas, par exemple, qu'un fournisseur de services serve d'intermédiaire pour la transmission de ce matériel, par le biais d'un site Web ou d'un bavardoir, entre autres moyens, en l'absence de l'intention requise en l'occurrence en droit interne » : *Convention sur la cybercriminalité*, Rapport explicatif, *loc. cit.*, note 24, par. 105.

[222] Voir les articles 2 à 6 de la Convention. Les accès et interceptions illégales, l'atteinte à l'intégrité des données, l'atteinte à l'intégrité du système et les abus de dispositifs informatiques, comme la vente d'un mot de passe ou d'un code d'accès avec une intention frauduleuse, qui sont qualifiées d'infractions informatiques visent la protection de la confidentialité, de l'intégrité et de la disponibilité des données et des systèmes informatiques. L'« accès » désigne « la pénétration dans l'intégralité ou une partie quelconque d'un système informatique (matériel, composantes, données stockées du système installé, répertoires, données relatives au trafic et au

un fournisseur de services qui aide l'auteur du délit à transmettre un code malveillant ou un publipostage avec l'intention qu'une telle infraction soit commise peut engager sa responsabilité pénale[225]. Comme autre exemple, l'on retrouve la situation où l'intermédiaire aide l'auteur du crime à commettre l'infraction se rapportant au contenu[226]. Ainsi, l'intermédiaire qui aide l'auteur du crime à *posséder* de la pornographie juvénile[227] par le biais d'un système informatique avec l'intention qu'une telle infraction soit commise peut engager sa responsabilité pénale. Il en est de même pour l'intermédiaire qui aide l'auteur du crime à *produire*[228] ou à *diffuser* de la pornographie juvénile.

Deuxièmement, examinons le Protocole. Parallèlement à la Convention, le Protocole prévoit des dispositions qui ne s'appliquent qu'à l'auteur du crime, à l'exception d'une seule qui vise directement les intermédiaires techniques, à savoir celle liée à la complicité[229]. En vertu de cette disposition, l'intermédiaire peut engager

---

contenu) » : *Convention sur la cybercriminalité*, Rapport explicatif, *loc. cit.*, note 24, par. 46. Toutefois, est exclu de la définition le simple envoi de messages électroniques ou de fichiers au système informatique; L'article 2 concerne les infractions visant à mettre en danger le système informatique ou attenter à la sécurité des données informatiques : *Convention sur la cybercriminalité*, Rapport explicatif, *loc. cit.*, note 24, par. 46.

[223] L'article 4 concernant l'atteinte à l'intégrité des données protège « l'intégrité, le bon fonctionnement ou le bon usage de données ou programmes informatiques ».

[224] L'article 5 de la Convention concernant l'atteinte à l'intégrité du système vise à pénaliser l'entrave intentionnelle et grave à l'usage légitime de systèmes informatiques, y compris de systèmes de télécommunications, en utilisant ou en influençant des données informatiques.

[225] Toutefois, il faut préciser qu'un fournisseur de services qui n'a pas l'intention criminelle ne peut être tenu responsable au titre de la section.

[226] L'infraction se rapportant au contenu qui est sanctionnée à l'article 9 de la Convention prétend accroître le niveau de protection accordée aux enfants contre la production, la possession et la diffusion illicites de pornographie juvénile sur le système informatique. L'objectif de cette infraction est le contrôle de la production de la pornographie juvénile. Certes, l'on s'accorde pour reconnaître que la possession de matériel explicite et le développement de pratiques en lignes qui s'y rattachent, telles que l'échange d'idées entre pédophiles, contribuent à renforcer la demande, ce qui encourage et facilite la commission d'infractions à l'encontre d'enfants. Afin d'empêcher que l'on ne s'expose à une accroissance de la demande, l'incrimination de divers actes illicites se rapportant à la pornographie juvénile était de mise : *Convention sur la cybercriminalité*, Rapport explicatif, *loc. cit.*, note 24, par. 93

[227] Le paragraphe 2 précise que le terme « pornographie juvénile » comprend toute matière pornographique représentant de manière visuelle: a) un mineur se livrant à un comportement sexuellement explicite; b) une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite; c) des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.
En outre, les trois types de matériels définis au paragraphe 2 incluent respectivement : i) des représentations d'un abus d'enfant réel; ii) des images illustrant « une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite » iii) et des images réalistes qui ne représentent pas d'enfant véritable se livrant à une activité sexuellement explicite : *ibid*, par. 101.

[228] L'article 9 de la Convention incrimine la production de la pornographie juvénile, la diffusion, l'offre ou la mise à disposition –notamment par « *la création ou la compilation d'hyperliens vers des sites pédophiles en vue de faciliter l'accès à la pornographie juvénile* ».

[229] En vertu de l'article 7 du Protocole qui énonce ce qui suit : « Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, en vertu de son droit interne, lorsqu'il est commis intentionnellement et sans droit, le fait d'aider à perpétrer une infraction telle que définie dans ce Protocole, ou d'en être complice, avec l'intention qu'une telle infraction soit commise ».

sa responsabilité pénale s'il pose un acte qui est de nature à aider l'auteur du crime dans la commission de l'une des infractions listées dans le Protocole[230], avec l'intention qu'une telle infraction soit commise[231]. Selon le rapport explicatif, pour que la responsabilité de l'intermédiaire soit engagée à titre de complice, il doit non seulement exercer un certain contrôle sur l'activité en question mais il doit également avoir connaissance du caractère illicite de l'activité[232]. À cet égard, l'on peut donner plusieurs exemples de situations qui illustrent la nécessité de retrouver de façon cumulative les critères de contrôle et de connaissance comme éléments constitutifs d'une infraction. À titre d'exemple, prenons le cas où l'intermédiaire aide l'auteur du crime à procéder à la diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques[233], notamment par la création ou la compilation d'hyperliens. Ainsi, l'intermédiaire qui aide l'auteur du crime à échanger du matériel dans un *chat-room* ou à distribuer dans des newsgroups ou des forums de discussion du matériel illicite avec l'intention qu'une telle infraction soit commise peut engager sa responsabilité pénale. Comme autre exemple, l'on retrouve la situation où l'intermédiaire aide l'auteur du crime à proférer des menaces avec motivation raciste et xénophobe[234] par le biais d'un système informatique et dirigée contre une personne ou un groupe de personne au motif d'appartenance à un groupe caractérisé par la race, la couleur, l'ascendance ou l'origine nationale ou ethnique, ou la religion. L'intermédiaire qui aide l'auteur du crime à diffuser de l'information contenant des

---

[230] Les infractions d'aide et de complicité sont prévues à l'article 7 du Protocole qui fait référence aux articles 3 à 6 du Protocole.

[231] Parallèlement à la Convention, le Protocole exige l'intention de commettre l'acte de complicité ainsi que l'intention que soit commise l'une des infractions qui sont prévues aux 3 à 6 du Protocole.

[232] Le rapport explicatif énonce ce qui sui : « [a]insi, par exemple, bien que la transmission par le biais de l'Internet de matériel raciste et xénophobe requière l'assistance de fournisseurs de services agissant comme intermédiaires, un fournisseur de services qui n'a pas d'intention criminelle ne peut être tenu responsable au titre de cette section » : *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, Rapport explicatif, *loc. cit.*, note 28, par. 45.

[233] L'utilisation du terme « du public » exclut expressément l'idée de toute communication privée. La question de savoir si la communication est de nature privée doit être examinée à la lumière de l'intention spécifique de l'émetteur du message de le transmettre à une personne spécifique, laquelle sera établie en tenant compte de plusieurs facteurs, tels que le contenu du message, la technologie employée, les mesures de sécurité appliquées et le contexte dans lequel celui-ci est transmis. La diffusion du matériel illicite doit se faire au public, par exemple, par l'échange du matériel dans un *chat-room* ou la distribution dans des newsgroups ou des forums de discussion : *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, Rapport explicatif, *loc. cit.*, note 28, par. 29-31.

[234] L'infraction est prévue à l'article 4 du Protocole : *ibid*, par. 33, 35. La menace doit prendre la forme d'une intimidation qui entraîne chez la personne victime une crainte résultant de la commission d'une infraction pénale grave. La menace qui est exprimée lors d'une communication privée est aussi couverte par cette disposition : *ibid*, par. 35. Cette disposition donne libre choix aux États de déterminer ce qui constitue une infraction pénale grave : *ibid*, par. 34.

propos racistes et xénophobes par voie électronique (courrier électronique) ou par le biais de « *Messenger* », de manière à entraîner chez la victime une crainte de violation de l'intégrité physique de sa personne (avec l'intention qu'une telle infraction soit commise) peut engager sa responsabilité pénale.

Après l'analyse de la Convention et du Protocole, il y a lieu de faire les constatations suivantes. L'on a observé que seules les dispositions[235] qui traitent de la complicité se trouvent directement applicables aux intermédiaires techniques. L'on a constaté qu'aux termes de ces dispositions visant la complicité, l'on doit retrouver de façon cumulative les notions de connaissance et de contrôle pour pouvoir imputer une certaine responsabilité pénale aux intermédiaires techniques. L'on a vu que la notion de contrôle fait référence au fait d'apporter une aide à l'auteur du crime dans la commission du crime alors que la notion de connaissance se rapporte au fait d'avoir l'intention qu'une infraction prévue au Protocole ou à la Convention soit commise. L'on a remarqué que ces deux textes internationaux traitent de la notion de contrôle selon une compréhension qui est uniforme à l'égard de tous les intermédiaires techniques. L'on a vu que la Convention et le Protocole se concentrent davantage sur les différents types d'activités pouvant être commis sur Internet que sur les intermédiaires eux-mêmes[236], étant donné qu'ils constituent tout d'abord un instrument de répression pénale et ce, contrairement à la *Directive sur le commerce électronique*, aux lois américaine, québécoise et française qui se concentrent davantage sur les différents acteurs d'Internet.

En conclusion, il faut reconnaître que la Convention et le Protocole ne sont pas de grande utilité pour faire des nuances entre les différents intermédiaires techniques[237]. Ce constat n'empêche toutefois pas de comparer ce texte avec les autres

---

[235] C'est-à-dire l'article 11 de la Convention et l'article 7 du Protocole.

[236] Ces deux textes décrivent de façon détaillée toutes les infractions répertoriées, témoignant ainsi d'un souci d'assurer une plus grande protection du public face aux risques d'atteintes diverses. Alors que les autres instruments juridiques nationaux et internationaux ne décrivent pas séparément les différents types d'activités illicites. Par ailleurs, l'on n'observe pas de complémentarité dans les autres instruments juridiques. L'existence d'une telle complémentarité démontre le souci du législateur d'informer le public sur la gravité de ces infractions pouvant être commises par des intermédiaires techniques alors que les autres instruments juridiques nationaux et internationaux ne recoupent ces infractions que sous l'appellation « *informations* » ou « *activités illicites* ».

[237] Malgré le constat suivant lequel le principe de contrôle s'articule de façon homogène pour tous les intermédiaires techniques, ces instruments juridiques comportent tout de même de multiples avantages. Tout d'abord, ils prêtent à une codification qui se veut compatible avec les nouvelles technologies et accessible à cet environnement électronique qui se complexifie au fur et à mesure que la criminalité informatique et les nouvelles

lois et textes internationaux afin de tirer des conclusions pertinentes, notamment sur la nature des activités illicites commises sur Internet. Par conséquent, malgré une description homogène du principe de contrôle applicable à l'égard de tous les intermédiaires techniques, la Convention et le Protocole comprennent tout de même la notion de contrôle comme un pré-requis à l'imputation de responsabilité des intermédiaires techniques.

B) La *Directive sur le commerce électronique*

Dans cette section, il convient d'analyser les différentes dispositions[238] de la *Directive sur le commerce électronique* qui traitent de la notion de contrôle mais suivant une compréhension nuancée selon les différents intermédiaires techniques visés[239]. Plus précisément, il s'agit de voir dans quelle mesure la *Directive sur le commerce électronique* traite de la notion de contrôle pour chacun des intermédiaires techniques et ce, en faisant les principales distinctions avec les autres instruments juridiques nationaux et internationaux.

Si la *Directive sur le commerce électronique* comprend un principe de contrôle[240] qui prend sa coloration à partir du rôle assumé par chacun des intermédiaires techniques, c'est qu'il y a tout de même un principe global selon lequel chacun ne doit pas dépasser la ligne séparant le caractère passif de son rôle exercé dans la chaîne de communication de l'information. Autrement dit, qu'il s'agisse d'une activité de simple transport, de stockage de l'information ou d'hébergement de données[241], le principe étant que l'intermédiaire en question doit *a priori* tenir un rôle

---

manières de commettre des crimes s'accroissent. Le droit prête une nouvelle façon de faire, une nouvelle façon de réfléchir sur les nouvelles réalités qui s'affichent dans cet environnement nouveau qui se veut de plus en plus « *dangereux* » mais, en même temps, sécuritaire, pour ceux qui sont capables de s'y adapter.

[238] La *Directive sur le commerce électronique* entend régler les cinq questions suivantes posées par le commerce électronique: régime d'établissement de l'ISP; réglementation de la communication commerciale; conclusion en ligne de contrats; responsabilité des intermédiaires; mise en oeuvre (adoption de codes de conduite, règlement des différends, etc.).

[239] La directive qui a été adoptée en mai 2000 par le Parlement européen. Directive *2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur* (ci-après citée « directive sur le commerce électronique »), *loc. cit*, note 15.

[240] C'est dans la section 4 de la directive que l'on retrouve les dispositions qui traitent de la responsabilité des prestataires de services : c'est-à-dire les articles 12 à 15 de la *Directive sur le commerce électronique.*

[241] Article 12 de la *Directive sur le commerce électronique.*

passif dans la chaîne de communication, c'est-à-dire que ses agissements ne doivent pas être de la nature de l'exercice d'un pouvoir éditorial.

Dans le cas contraire, la *Directive sur le commerce électronique* prévoit expressément que le prestataire de services sera tenu responsable du préjudice résultant des informations fournies par le destinataire du service lorsque ce dernier agit sous le contrôle ou l'autorité du prestataire de services[242]. Ainsi, l'on présumera qu'il exerce un certain contrôle éditorial sur le contenu de l'information diffusée lorsque l'on convient qu'il a le pouvoir d'enjoindre cette personne à exécuter des fonctions. Par conséquent, l'intermédiaire ne doit exercer aucune forme de contrôle sur le contenu de l'information, que ce soit avant ou pendant la transmission de l'information, à défaut de quoi sa responsabilité risque d'être engagée.

La *Directive sur le commerce électronique* organise le principe de contrôle avec des variations qui se dessinent à partir du rôle joué par chacun des intermédiaires concernés dans la transmission de l'information et ce, contrairement à la *Convention sur la cybercriminalité* et parallèlement aux autres instruments juridiques nationaux et internationaux. Dans ce sens, il faut présenter les dispositions qui se rapportent à chacun des intermédiaires techniques, à savoir le transmetteur, le prestataire de services de *caching* et l'hébergeur.

Premièrement, il y a lieu d'étudier la disposition[243] régissant la responsabilité du transmetteur sous l'angle du critère de contrôle. Le transmetteur a pour fonction *de transmettre, sur un réseau de communication, des informations fournies par le destinataire du service ou de fournir un accès au réseau de communication.* Son rôle est donc comparable à un fournisseur de services Internet, tels que Sympatico ou Vidéotron[244]. La *Directive sur le commerce électronique* énonce les situations dans lesquelles la responsabilité de cet intermédiaire peut être envisagée. Comme première condition, la *Directive sur le commerce électronique* énonce que le prestataire de service ne doit pas être à l'origine de la transmission de l'information à contenu

---

[242] En vertu de l'article 14 de la *Directive sur le commerce électronique.*

[243] En vertu de l'article 12 de la *Directive sur le commerce électronique.*

[244] L'article 12 de la *Directive sur le commerce électronique* énonce que « les activités de transmission et de fourniture d'accès visées au paragraphe 1 englobent le stockage automatique, intermédiaire et transitoire des informations transmises, pour autant que ce stockage serve exclusivement à l'exécution de la transmission sur le réseau de communication et que sa durée n'excède pas le temps raisonnablement nécessaire à la transmission ».

potentiellement dommageable[245]. Ce qui signifie qu'il ne doit pas pouvoir décider de ce qui sera envoyé ou transmis, sur un réseau de communication, à son destinataire. Puisqu'en étant à l'origine de l'information litigieuse, il se retrouverait ainsi à exercer un contrôle physique sur l'information. Comme autre condition qui réfère cette fois au contrôle du sens, l'on retrouve l'exigence selon laquelle le transmetteur ne doit pas modifier le contenu de l'information à transmettre[246]. L'obligation de ne pas perturber le cours de traitement des données comprend entre autres, l'obligation pour l'intermédiaire de ne pas excéder le temps raisonnablement nécessaire à l'exécution de la transmission de l'information[247]. Comme troisième condition, il y a également la nécessité pour le transmetteur de ne pas sélectionner le destinataire de la transmission[248]. Ces trois conditions se dégagent également des lois française et québécoise[249]. La faculté de choisir la personne à qui sera envoyée l'information se rapporte au contrôle physique, affectant le cours de traitement de l'information. Par conséquent, la *Directive sur le commerce électronique* impose au transmetteur une obligation négative, celle de ne pas agir, tant qu'il n'a pas eu effectivement connaissance du caractère illicite de l'activité en question. Ainsi, le fait pour ce dernier de poser des gestes qui dérivent d'un pouvoir de contrôle devient source de responsabilité pour celui-ci. Ces gestes peuvent parfois découler d'un contrôle physique et parfois d'un contrôle du sens.

Deuxièmement, il y a lieu d'examiner comment la notion de contrôle s'articule dans la disposition qui prévoit la responsabilité de l'intermédiaire qui fait le stockage de l'information sur un réseau de communication dans le seul but de rendre plus efficace leur transmission ultérieure[250]. Le rôle de cet intermédiaire est comparable à celui du transmetteur puisqu'il n'intervient que lors de la transmission de l'information transitant d'un point à un autre du réseau. Contrairement aux lois française et québécoise qui posent un régime d'exonération conditionnelle de responsabilité, la *Directive sur le commerce électronique* énonce que le prestataire qui conserve

---

[245] En vertu de l'article 12 de la *Directive sur le commerce électronique*.
[246] En vertu des articles 12 de la *Directive sur le commerce électronique*.
[247] En vertu de l'article 12 de la *Directive sur le commerce électronique*.
[248] En vertu de l'article 12 de la *Directive sur le commerce électronique*.
[249] En vertu de l'article 9 de la *LCEN* qui modifie l'article L32-3-3 du *Code des postes et des communications électroniques* et de l'article 36 de la *LCCJTI*.
[250] En vertu de l'article 13 de la *Directive sur le commerce électronique*.

l'information dans le seul but de rendre plus efficace la transmission ultérieure de l'information est *a priori* non-responsable, à condition de ne pas se retrouver dans l'une des situations visées. Tout d'abord, parallèlement au transmetteur, cet intermédiaire peut engager sa responsabilité notamment s'il modifie l'information transmise. Modifier le contenu de l'information implique un contrôle sur le sens de l'information. Ensuite, le fait pour ce dernier de ne pas se conformer aux conditions d'accès à l'information et aux règles concernant la mise à jour de l'information, indiquées d'une manière largement reconnue par les entreprises peut être source de responsabilité pour celui-ci. Il en est de même pour celui qui entrave le cours de l'utilisation licite des données informatiques[251]. Ainsi, celui qui ne se conforme pas aux conditions d'accès ou fait une utilisation à des fins autres que celles qui sont strictement vouées à l'exécution de la transmission de l'information pose un geste qui découle d'un contrôle physique. Enfin, il peut être tenu responsable s'il n'agit pas promptement pour retirer l'information qu'il a stockée ou pour en rendre l'accès impossible dès qu'il est mis au courant de la présence d'activités illicites sur le réseau[252]. Cette dernière condition se rattache à un contrôle physique car l'omission de prendre des mesures afin de retirer ce qui est illicite ou d'en interdire l'accès suppose la présence d'un certain pouvoir sur la réalisation de l'activité en question. Rappelons que ces conditions s'inscrivent également dans les lois française et québécoise[253]. Ainsi, la notion de contrôle ressort de ces cinq situations qui constituent alors des conditions d'ouverture de la responsabilité de cet intermédiaire. Les situations présentent cette notion comme apparaissant tantôt dans sa forme physique et tantôt dans sa forme intellectuelle.

Ttroisièmement, la notion de contrôle ressort également de la disposition de la *Directive sur le commerce électronique* visant la responsabilité de l'hébergeur[254]. Son rôle consiste en un *stockage des informations fournies par un destinataire du service* sur le réseau Internet. Plus concrètement, l'hébergeur est celui qui héberge dans des serveurs des fichiers et autres documents émanant des tiers. Il peut s'agir d'un maître

---

[251] En vertu de l'article 13 de la *Directive sur le commerce électronique.*
[252] En vertu de l'article 13 de la *Directive sur le commerce électronique.*
[253] En vertu de l'article 9 de la *LCEN* qui modifie l'article L32-3-4 du *Code des postes et des communications électroniques* et de l'article 37 de la loi québécoise.
[254] En vertu de l'article 14 de la *Directive sur le commerce électronique.*

de blogue qui conserve sur le blogue des documents publiés par des tiers. Contrairement à loi française qui établit expressément un régime de responsabilité pénale applicable à l'hébergeur[255], la *Directive sur le commerce électronique* pose principalement un régime de responsabilité civile, tout en donnant la possibilité aux États de prévoir des sanctions qui doivent être effectives, proportionnées et dissuasives[256]. Il faut en outre mentionner que la *Convention sur la cybercriminalité* ne traite pas séparément de la responsabilité de l'hébergeur, se contentant d'établir une distinction qu'à l'égard du fournisseur de services Internet et ce, tout comme la loi américaine et contrairement à la *Directive sur le commerce électronique* et la loi française. À la différence des lois québécoise et française qui énoncent un régime d'exonération conditionnelle de responsabilité, la *Directive sur le commerce électronique* pose que l'hébergeur est *a priori* non-responsable mais qu'il peut engager sa responsabilité dans certaines situations[257]. Le libellé de la disposition[258] reprend les mêmes termes que la loi française. Parallèlement aux lois québécoise, française et américaine, la *Directive sur le commerce électronique* fait référence à cette notion de manière implicite[259]. Elle énonce que le prestataire en question ne doit pas être au courant ni des activités ou informations illicites ni des faits ou circonstances donnant lieu à croire que l'activité ou l'information est de façon apparente illicite[260]. Ce qui suppose que le prestataire ne doit exercer aucun contrôle sur l'information ou activité en question. Au deuxième alinéa de la même disposition[261], la *Directive sur le commerce électronique* dispose que dès qu'il a connaissance de l'illicéité de l'information ou activité en question, l'hébergeur doit agir promptement pour retirer ces informations ou rendre l'accès à celle-ci impossible. À cet égard, le maître de blogue qui omet de retirer l'information litigieuse ou de rendre l'accès impossible alors qu'il a découvert que le contenu publié par le tiers contient des propos litigieux sera alors tenu responsable au sens de cette disposition. Puisque son inaction permet la réalisation de l'activité illicite et se rattache à l'idée de contrôle qu'il exerce sur

---

[255] Article 6-I-3 de la *LCEN*. Alors que la *Directive sur le commerce électronique* ne le prévoit qu'implicitement.
[256] La *Directive sur le commerce électronique* le prévoit par le biais de son article 20.
[257] En vertu de l'article 14 de la *Directive sur le commerce électronique*.
[258] En vertu de l'article 14 de la *Directive sur le commerce électronique*.
[259] En vertu des articles 22 de la *LCCJTI*, 6-I-2 de la *LCEN* et de l'article 230(c)(2) de *Communications Decency Act*.
[260] En vertu de l'article 14 de la *Directive sur le commerce électronique*.
[261] *ibid.*

déroulement de l'activité en question. Alors que la notion de contrôle se manifeste de manière explicite dans les dispositions visant le transmetteur et l'intermédiaire qui fait le stockage de l'information sur un réseau de communication dans le seul but de rendre plus efficace leur transmission ultérieure, elle apparaît de manière implicite dans la disposition qui traite de l'hébergeur.

En résumé, la *Directive sur le commerce électronique* qui reconnaît le rôle généralement passif des intermédiaires techniques organise un cadre juridique s'énonçant *a priori* par un régime de responsabilité limitée, et ensuite, de responsabilité, lorsqu'il advient une série d'indices « *sérieuses* » qui portent à conclure que le rôle de l'intermédiaire ne peut plus se qualifier de « *passif* ». La *Directive sur le commerce électronique* se concentre davantage sur les intermédiaires en tant que tels alors que la *Convention sur la cybercriminalité* met davantage l'emphase sur les diverses catégories d'infractions. Elle retient une compréhension nuancée du principe de contrôle selon les intermédiaires concernés. Alors qu'elle apparaît de manière explicite pour le transmetteur et l'intermédiaire fournissant des services de *caching*, elle se manifeste de manière implicite pour l'hébergeur. Par ailleurs, la notion de contrôle prend la forme d'un contrôle physique ou d'un contrôle du sens. La forme de contrôle exercée par l'intermédiaire est modulée selon le type d'actes posés par chacun. Lorsque le geste posé, qu'il soit passif[262] ou actif, affecte le contenu de l'information, l'intermédiaire exerce un contrôle du sens sur l'information. Alors que lorsque l'acte posé se rapporte à un pouvoir de retirer l'information ou d'en empêcher l'accès afin de faire cesser la commission de toute activité illicite, il s'agit d'un contrôle physique. Le fait pour l'intermédiaire de poser un geste qui se rattache à un contrôle physique ou à un contrôle du sens est générateur de responsabilité pour ce dernier[263]. Enfin, à la différence de la loi québécoise, la *Directive sur le commerce électronique* reste toutefois silencieuse sur la responsabilité découlant des liens

---

[262] Il faut préciser que même en la présence d'un état de passiveté, l'intermédiaire peut se retrouver dans une situation de responsabilité si l'on juge que ce geste découle d'un certain contrôle sur l'activité. Ainsi, le fait de ne pas se conformer pas aux règles de mise à jour de l'information peut être source de responsabilité pour ce dernier.

[263] Elle prévoit une mesure donnant la possibilité aux États d'imposer au prestataire technique une obligation de prévention avant même qu'il ne reçoive une notification indiquant la présence d'activités ou informations illicites par le biais de ses services. Cette mesure permet à l'intermédiaire de mettre un terme à la violation ou à empêcher le risque de la survenance d'activités illicites sur le réseau Internet. La mise en œuvre de telles mesures de sécurité permettra aux prestataires de se prémunir contre d'éventuels recours en responsabilité civile ou pénale provenant d'une tierce partie. Voir les articles 12(3), 13(2) et 14(3) de la *Directive sur le commerce électronique*.

hypertextes, répertoires, moteurs de recherche et autres outils servant à localiser de l'information en ligne.

Par conséquent, le principe de contrôle s'annonce comme un critère d'imputabilité qui se montre plus aiguisé que celui que l'on retrouvait dans le texte précédent mais toujours incomplet puisque ne couvrant pas la responsabilité de cet intermédiaire.

Après avoir décrit la notion de contrôle à partir du texte européen, passons maintenant à la loi française.

C) La *Loi pour la confiance dans l'économie numérique*

Dans cette section, il convient d'examiner la *Loi pour la confiance dans l'économie numérique* (ci-après appelé : « *LCEN* »)[264] afin de dégager le principe de contrôle, de manière à soulever des nuances entre les différents intermédiaires techniques en ce qui concerne leur régime de responsabilité. La *LCEN* englobe la notion de contrôle dans les dispositions qui concernent les intermédiaires techniques, à savoir l'hébergeur, le transmetteur et l'intermédiaire assurant une activité de stockage automatique dans le seul but de rendre plus efficace leur transmission ultérieure.

Tout d'abord, il faut voir comment se manifeste la notion de contrôle dans la disposition traitant de l'hébergeur[265]. Le rôle du prestataire consiste à « *assurer, même à titre gratuit, pour mise à disposition du public par services de communications en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute*

---

[264] La *LCEN* est la transposition de la Directive 2000/31/CE. La transposition n'a été effective que le 21 juin 2004 et la *LCEN* a parue au JO n° 143 du 22 juin 2004. La raison pour laquelle la *LCEN* a pris du retard est la présence de virulentes oppositions de la part des acteurs d'Internet, notamment les fournisseurs de services Internet. Alors qu'elle aurait dû être effective le 17 janvier 2002, n'a été que : *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, *loc. cit.*, note 16. La loi française, à la différence de la *Directive sur le commerce électronique*, crée un régime d'exonération conditionnelle de responsabilité Toutefois, parallèlement à la *Directive sur le commerce électronique*, la loi française prétend instaurer un régime de responsabilité devant s'appliquer tant sur le plan civil que pénal et ce, contrairement à la *Convention sur la cybercriminalité* qui ne traite que de la responsabilité pénale. Cependant, tout comme la *Directive sur le commerce électronique* et loi américaine, la loi française ne prévoit aucun régime de responsabilité en ce qui concerne l'intermédiaire offrant des services de références à des documents technologiques. De plus, la *LCEN* reprend les principes du droit communautaire en matière de commerce électronique qui sont déjà établis dans la *Directive sur le commerce électronique*, tels que le principe de proportionnalité, de la liberté d'expression, de contrôle de la société de l'information, le principe du secret des communications : les considérants 10, 9, 22 et 15 de la *Directive sur le commerce électronique*. En ce sens, tout comme la *Directive sur le commerce électronique* et *la Convention sur la cybercriminalité*, la *LCEN* entend établir un juste équilibre entre la protection des droits humains fondamentaux et le droit à la liberté de l'expression. C'est dans cette optique de pondération d'intérêts divergents que la *LCEN* se prononce sur la question de la responsabilité des intervenants de la communication électronique sous l'angle du principe de contrôle.

[265] En vertu de l'article 6-I-2° de la *LCEN*.

nature fournis par des destinataires de ces services »[266]. La *LCEN* prévoit que la responsabilité civile ou pénale de l'hébergeur peut être engagée s'il omet de retirer le contenu litigieux ou en rend l'accès impossible alors qu'il a été dûment informé de son caractère illicite[267]. En l'espèce, la notion de contrôle se dégage explicitement du libellé de cette disposition et ce, contrairement à la *Directive sur le commerce électronique*. Il faut préciser que le principe de contrôle applicable à l'hébergeur est énoncé de manière encore plus générale dans la *Convention sur la cybercriminalité*. L'omission de retirer le contenu litigieux ou d'en rendre l'accès impossible permettant la réalisation de l'activité illicite suppose que l'intermédiaire détienne un certain contrôle sur le déroulement de cette activité. Ce qui l'empêchera de se qualifier à titre d'hébergeur. À cet égard, dans une décision du 19 octobre 2007[268], le TGI de Paris a tenu responsable *Google* pour ne pas avoir retiré *efficacement* le contenu litigieux, bien qu'il soit dûment informé de son caractère litigieux. Le jugé a considéré que l'hébergeur aurait dû instaurer une mesure technique empêchant la réapparition en ligne de la matière litigieuse. Ainsi, cette décision enseigne que l'hébergeur doit, afin de remplir son obligation adéquatement, retirer le contenu de façon définitive.

Par ailleurs, la *LCEN* dispose que la responsabilité de l'hébergeur peut également être engagée si le destinataire qui exerce une activité illicite agit sous l'autorité ou le contrôle de cet intervenant[269]. Pour que l'obligation de l'hébergeur puisse naître, il faut que les activités ou le contenu en question aient effectivement un caractère illicite, qui s'obtient, soit par un tiers indépendant ou un juge, sur le fondement du caractère « manifestement » illicite de l'activité ou de l'information en question[270]. Le terme « *autorité* » employé par la *LCEN* fait directement référence au lien de subordination existant dans un contrat de travail tandis que celui de « *contrôle* » est plus flou. Selon Lionel Thoumyre, il se rattache à une idée de pouvoir plutôt qu'à celle de surveillance[271]. Ainsi, l'hébergeur ne pourrait être qualifié à titre

---

[266] *ibid.*
[267] *ibid.*
[268] *Google* c./ *Zadig productions, précitée*, note 142.
[269] En vertu de l'article 6-I-2° de la *LCEN*.
[270] Dans la décision n° 2004-496 DC du 10 juin 2004, le Conseil constitutionnel a émis une réserve d'interprétation qui est à l'effet que : « *ces dispositions ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge* ».
[271] Lionel THOUMYRE, « Précisions contrastées sur trois notions clés relatives à la responsabilité des hébergeurs », *Revue Lamy droit de l'immatériel*, février 2008, n. 35, p. 18.

d'éditeur seulement parce qu'il choisit un certain type de structure de présentation de son site Web. C'est d'ailleurs l'avis exprimé dans le rapport parlementaire sur l'application de la *LCEN* : « *un fournisseur d'hébergement est nécessairement conduit à structurer l'information qu'il stocke sur son ou ses serveurs [...] La loi ne fait d'ailleurs pas dépendre la qualité d'hébergeur de la manière dont le service d'hébergement est organisé* »[272]. La jurisprudence majoritaire qui est au même effet retient que le type d'architecture imposé par le site Web et le fait de tirer un revenu substantiel de la vente des espaces publicitaires ne changent en rien à son rôle de simple hébergeur. À cet égard, dans les deux décisions rendues le 15 avril 2008 où le site *Dailymotion* est le défendeur[273], le TGI de Paris a qualifié le site en question d'hébergeur, en précisant que « *le fait de structurer les fichiers mis à la disposition du public selon un classement choisi par le seul créateur du site [et] la commercialisation d'espaces publicitaires ne donne[nt] pas à ce dernier la qualité d'éditeur tant qu'il ne détermine pas les contenus des fichiers mis en ligne* »[274]. Il en ressort de ces décisions qu'un site qui *contrôle la qualité générale des contenus* afin d'empêcher qu'un certain type de contenus ne soit diffusé exerce un contrôle purement technique. Alors qu'un site qui *contrôle le destinataire des services* afin de décider de la teneur des contenus produits par le destinataire en question exercera un contrôle intellectuel[275]. À titre d'exemple, il peut s'agir de l'hébergeur qui ordonne au destinataire du service d'effectuer une tâche selon les modalités qu'il fixe. On le qualifiera dans le premier cas d'hébergeur alors que dans le second cas, d'éditeur. Or, il y a une certaine tendance à considérer le pouvoir d'agencement et d'organisation des flux RSS des sites communautaires comme un facteur permettant de qualifier l'acteur d'éditeur[276]. À cet égard, dans une ordonnance de référée[277], le TGI

---

[272] Rapport d'information n° 627 sur la mise en application de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, présenté le 16 avril 2008 par les députés M. Jean Dionis du Séjour et Mme Corinne Erhel, p. 16, en ligne sur le site de l'Assemblée Nationale : < http://www.assemblee-nationale.fr/13/rap-info/i0627.asp > (visité le 11 février 2009) ; Julien TAÏEB, « Prestataires techniques de l'Internet : le sens des responsabilités », *loc. cit*, note 105.

[273] *Lafesse c. Dailymotion, précitée*, note 98 ; *Monsieur Omar Sy et Monsieur Fred Testot et autres* c/ *S.A. Dailymotion, précitée*, note 138.

[274] *ibid.*

[275] Julien TAÏEB, « Prestataires techniques de l'Internet : le sens des responsabilités », *loc. cit*, note 105 ; Benjamin MAY, « Responsabilité des acteurs du web 2.0 : l'histoire sans fin », *La Semaine Juridique Entreprise et Affaires* n° 17, 24 avril 2008, 1540.

[276] Voir également *M. O. D.* C./ *SARL Planète Soft, précitée*, note 109 ; *M. Olivier Dahan* c/ *M. Eric Duperrin, précitée*, note 109 ; *Jean-Yves L. dit LAFESSE / Myspace, précitée*, note 105.

[277] *Olivier Martinez* c./ *Bloobox Net, précitée*, note 108. Dans cette décision, la plateforme avait publié un lien vers le site célébrités-stars.blogspot.com indiquant que l'acteur Olivier Martinez était de nouveau en couple avec son ex-compagne.

de Paris devait se prononcer sur la qualification juridique de *Fuzz* qui est un site communautaire permettant aux usagers la publication et le partage de l'information diffusée ailleurs sur Internet. En l'espèce, l'internaute a pris l'information concernant Olivier Martinez sur un site Web et l'a faite automatiquement apparaître sur le site *Fuzz*. Le juge a considéré qu'« *en renvoyant au site celebrites-stars.blogspot.com, Fuzz.fr avait opéré un choix éditorial, de même qu'en agençant différentes rubriques* ». Pour ce dernier, « *l'acte de publication doit être compris non pas comme un simple acte matériel, mais comme la volonté de mettre le public en contact avec des messages de son choix* ». *Fuzz* « *doit donc être considéré comme un éditeur de service de communication au public en ligne* » et non comme un simple hébergeur. Il est difficile de voir dans quelle mesure *Fuzz* a eu véritablement l'intention de publier le contenu litigieux, étant donné que les messages diffusés étaient choisis par des utilisateurs et non par le maître du site[278].

Deuxièmement, le critère de contrôle apparaît dans la disposition visant le transmetteur[279]. Il s'agit de toute personne assurant une activité de transmission de contenus ou de fourniture d'accès à un réseau de télécommunications. Le libellé de la disposition est analogue à celui de la *Directive sur le commerce électronique* qui instaure un régime de responsabilité réduite a *priori* avec la possibilité d'engager par la suite la responsabilité de l'intermédiaire. La loi française énumère les situations qui peuvent engager la responsabilité civile ou pénale du transmetteur. Parmi ces situations, il y a notamment être à l'origine de la demande de transmission litigieuse, sélectionner le destinataire de la transmission ou sélectionner ou modifier les contenus faisant l'objet de la transmission. Ces cas de figure sont les mêmes que dans la *Directive sur le commerce électronique* et de la loi québécoise. Si la demande de transmission émane du transmetteur ou si ce dernier sélectionne le destinataire de la transmission, c'est qu'il exerce un contrôle physique sur le déroulement de l'activité en question. Si ce dernier a la faculté de sélectionner ou de modifier le contenu diffusé sur Internet, c'est qu'il possède un certain contrôle sur le contenu de l'information. Ainsi, les situations énumérées impliquent toutes un certain contrôle émanant de cet intermédiaire qui sera alors qualifié d'éditeur.

---

[278] Julien TAÏEB, « Prestataires techniques de l'Internet : le sens des responsabilités », *loc. cit*, note 105.
[279] En vertu de l'article 9-I de la *LCEN* (Art. L. 32-3-3 du *Code des postes et des communications électroniques*).

Troisièmement, l'on retrouve la notion de contrôle dans la disposition visant l'intermédiaire assurant une activité de stockage de l'information sur le réseau dans le seul but de rendre plus efficace leur transmission ultérieure[280]. Le rôle de cet intermédiaire est comparable à celui du transmetteur puisqu'il n'intervient que lors de la transmission de l'information. À cet égard, en raison de la nature passive de son rôle, il bénéficie d'une exonération de responsabilité qui est toutefois conditionnelle à ce qu'il conserve cet état de passiveté, à défaut de quoi il peut engager sa responsabilité. Son statut de simple intermédiaire peut alors changer s'il pose certains gestes affectant le contenu de l'information, notamment la modification du contenu de l'information illicite. Si l'intermédiaire en question a le pouvoir de modifier le contenu de l'information, c'est qu'il a également le pouvoir de remettre les choses dans l'état où elles étaient avant leur modification. Il ne sera non plus considéré en tant que simple intermédiaire s'il pose des actes découlant d'un contrôle physique, notamment en entravant le cours de l'utilisation licite et usuelle de la technologie pour obtenir des données ou en omettant de se conformer aux conditions d'accès de l'information et aux règles usuelles concernant leur mise à jour ou encore, en omettant d'agir avec promptitude pour retirer les contenus qu'il a stockés ou pour en rendre l'accès impossible, dès qu'il en a été informé de son caractère illicite[281]. Ainsi, si l'intervenant de la communication a le pouvoir d'enjoindre une personne à exécuter des tâches qui sont de nature à affecter le cours du traitement des données, c'est qu'il a également le pouvoir d'exiger de ce dernier qu'il retire tout contenu illicite ou cesse toute activité illicite. Que le contrôle s'effectue indirectement, à savoir par l'intermédiaire du destinataire du service ou plus directement, c'est-à-dire sur le contenu de l'information, l'on présume qu'il exerce un contrôle sur l'information ou activité en question et qu'il jouera un rôle d'éditeur. Contrôler signifie pouvoir changer de ce qui adviendra d'une chose dans le présent pour le futur. Le législateur français retient une compréhension de la notion de contrôle qui se rapproche de celle du législateur européen pour la *Directive sur le commerce électronique* et du législateur québécois et s'éloigne du législateur européen pour la *Convention de la cybercriminalité* qui ne contient qu'implicitement le principe de contrôle à l'égard de cet intermédiaire.

---

[280] En vertu de l'article 9-I de la *LCEN* (Art. L. 32-3-4 du *Code des postes et des communications électroniques*).
[281] En vertu de l'article 9-I de la *LCEN* (Art. L. 32-3-4 du *Code des postes et des communications électroniques*).

En résumé, l'on a vu que la loi française reproduit la *Directive sur le commerce électronique* en ce qui concerne les dispositions décrivant les rôles des trois intermédiaires, à savoir l'hébergeur, le transmetteur et l'archiveur. L'on a constaté que la détermination de la ligne séparant le statut de l'hébergeur et de l'éditeur n'était pas chose aisée dans la jurisprudence française qui a témoigné d'une incertitude marquée quant à l'interprétation de la disposition visant l'hébergeur. Le courant majoritaire a toutefois tranché en faveur d'un régime de responsabilité réduite de l'hébergeur qui exerce un contrôle technique sur le type de structure de présentation de son site Web. L'on a relevé deux types de contrôle dans les situations pouvant engager la responsabilité de chacun des intermédiaires techniques : un contrôle physique et un contrôle du sens. L'on a compris que lorsque l'intermédiaire posait des gestes se rapportant à un certain contrôle physique ou du sens, il ne pouvait plus être qualifié de simple intermédiaire, la nature de son rôle ayant en ce sens changé.

Par conséquent, la *LCEN* prend une orientation qui est semblable à la *Directive sur le commerce électronique* quant à l'interprétation de la notion de contrôle à l'égard de chacun des intermédiaires puisqu'elle considère que cette notion constitue un critère d'imputabilité des intermédiaires techniques. Toutefois, la loi française demeure silencieuse sur le régime de responsabilité imputable à l'intermédiaire assurant les services de références à des documents technologiques. D'ailleurs, la *LCEN* se montre plus précise sur la notion de contrôle que la *Convention sur la cybercriminalité* qui adopte une approche générale en créant une distinction uniquement à l'égard du transmetteur.

Après avoir examiné la loi française, analysons maintenant la loi américaine.

D) Le *Communications Decency Act*

La notion de contrôle se retrouve aussi dans la législation américaine dite *Communications Decency Act*[282]. Contrairement à la *Convention sur la cybercriminalité* et parallèlement à la loi québécoise, cette loi américaine ne s'applique donc pas sur le plan criminel. La disposition, qui est également appelée la clause du « *bon samaritain* », a été adoptée le 8 février 1996 par le Congrès américain dans le

---

[282] Voir, *supra*, note 18.

dessein d'amoindrir le niveau de responsabilité applicable aux fournisseurs de services Internet en matière de diffamation. À cet égard, le législateur américain, reconnaissant le potentiel normalisateur de la technologie, a donné une plus grande latitude aux fournisseurs de services Internet[283]. C'est pourquoi il a consacré toute une disposition régissant les méthodes de filtrage et de blocage du contenu offensant. Sur ce point, le *Communications Decency Act* reconnaît que ces services : *« [trad.] offrent un grand degré de contrôle aux usagers sur l'information qu'ils reçoivent, ainsi qu'un potentiel encore plus grand dans le futur, à mesure que la technologie se développera »*[284]. La politique des États-Unis est donc *« [trad.] d'encourager le développement de ces technologies qui optimisent le contrôle, par les individus, les familles et les écoles qui utilisent l'Internet et les autres services informatiques interactifs, sur l'information qu'ils reçoivent »*[285]. En outre, le *National Information Infrastructure Advisory Council* faisait la recommandation suivante, en décembre 1995, à l'*Infrastructure Information Task Force* : *« The government should not be in the business of regulating content on the Information Superhighway. It should defer to the use of privately provided filtering, reviewing and rating mechanisms, and parental supervision as the best means of preventing access by minors to inappropriate materials »*[286]. Le CDA a été en partie invalidé en juin 1997 par la Cour Suprême des États-Unis pour le motif de violation de la Constitution américaine et notamment de son 1er Amendement qui protège le « *free speech* »[287].

Le titre (c) de la section 230 de cette loi consacre un régime d'immunité en faveur des utilisateurs d'un service informatique interactif par laquelle ils ont une marge de manœuvre leur permettant d'enlever le matériel offensant sans crainte de supporter la responsabilité qui en découle[288]. La clause du « *bon samaritain* » permet

---

[283] Pierre TRUDEL et Karim BENYEKHLEF, « Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes », Mémoire présenté à la Commission de la Culture de l'Assemblée Nationale dans le cadre de son mandat sur l'étude du rapport quinquennal de la Commission d'accès à l'information, Montréal, Centre de Recherche en droit public, Université de Montréal, 1997, p. 24, en ligne sur : < https://papyrus.bib.umontreal.ca/dspace/bitstream/1866/71/1/0072.pdf > (visité le 22 juin 2008).

[284] *Communication Decency Act*, 47 U.S.C s. 230(a)(2).

[285] *Communication Decency Act*, 47 U.S.C s. 230(b)(3).

[286] *NIIAC Recommendation (December 12, 1995) to Secretary Ron Brown Regarding Content Regulation*, en ligne sur :< http://www.niiac-info.org/~niiac/content.html > (visité le 11 février 2009) ; Pierre TRUDEL et Karim BENYEKHLEF, « Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes », *loc. cit.*, note 283, p. 24.

[287] *Reno, Attorney General of the United States, et al.* c. *American Civil Liberties Union (ACLU) et al.*, *précitée*, note 55.

[288] *Telecommunications Act* de 1996, Pub. L. No. 104-104, tit. V, 110 Stat. 56, 133-43 (1996) (codifié dans les sections de 47 U.S.C.). Le *CDA* est situé dans le titre V du *Telecommunications Act* de 1996, qui est amendé par le *Communications Act* de 1934 : Melissa A. TROIANO, « Comments –The New Journalism? Why the Traditional

aux utilisateurs d'un service informatique interactif d'exercer un certain contrôle sur les contenus litigieux circulant via leurs installations car, en vertu de cette disposition, ils peuvent, de leur propre initiative, prendre des moyens en vue de supprimer le contenu litigieux ou de restreindre l'accès ou la disponibilité de matériel qu'ils considèrent obscène, excessivement violent ou autrement offensant. En effet, bien que la loi ne leur impose aucune obligation de supprimer les contenus illicites circulant par le biais de leurs réseaux, ils peuvent décider de le faire volontairement et à partir de ce moment, ils seront tout simplement considérés comme agissant en bon samaritain et bénéficieront d'une immunité prévue par la loi[289].

La jurisprudence applique le régime d'immunité en faveur des fournisseurs d'accès Internet. À cet égard, dans l'arrêt *Kenneth M. Zeran* v. *America Online Inc.*,[290] les juges ont exonéré, sur le fondement de *Communication Decency Act* de 1996, *America Online* de toute responsabilité en ce qui concerne les informations diffamatoires publiées sur son serveur commercial et émanant d'un tiers, en estimant que le fournisseur d'accès n'avait aucune obligation de les supprimer de son réseau et s'il décide de le faire, il serait tout simplement considéré comme un « *bon samaritain* ». Cet arrêt établit également une distinction entre l'intermédiaire qui offre des services de connexion et les autres diffuseurs d'informations, comme par exemple, les éditeurs de journaux, magazines et télévision. À cet égard, l'auteure Melissa A. Troiano qui critique chaudement le libellé de cette disposition dans son article[291] qualifie d'artificielle la distinction existant entre les utilisateurs d'un service informatique interactif qui publient des messages diffamatoires et les autres diffuseurs d'informations, comme par exemple, les éditeurs de journaux, magazines et télévision.

Defamation Laws Should Apply to Internet Blogs? (2007) 56 *American University Law Review* 1450, en ligne sur: < http://www.wcl.american.edu/journal/lawrev/55/troiano.pdf?rd=1 > (visité le 21 juin 2008). La clause prévoit que: « *no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider* ».

[289] *Communication Decency Act*, 47 U.S.C s. 230(c)(1) énonce ce qui suit : « TREATMENT OF PUBLISHER OR SPEAKER- No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. ». La Loi oblige également les manufacturiers de télévision à installer des équipements qui permettront aux téléspectateurs de bloquer certaines émissions, en raison de leur qualification : Pierre Trudel et Karim Benyekhlef, « Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes », *loc. cit.*, note 283, p. 24.

[290] U.S. District Court, E.D. Virginia, 958 F.Supp. (1997); U.S Court of Appeals, 4th Circuit, CA-96-1564-A, 129 F.3d 327 (1997); 118 S. Ct. 2341 (1998), rejeté. Cet arrêt apparaît tout de suite après l'adoption de la disposition.

[291] Il faut noter que l'opinion de cette auteure est minoritaire et ne représente pas le courant majoritaire. Ainsi, elle commente ce qui suit : « [...] While newspaper editors receive strict liability for this sort of behaviour the *CDA* ensured that interactive computer services would receive no liability at all. »: Melissa A. TROIANO, « Comments – The New Journalism? Why the Traditional Defamation Laws Should Apply to Internet Blogs? », *loc. cit.*, note 288.

Quoi qu'elle en soit, cette distinction semble à première vue difficile à établir par les tribunaux américains. Dans la décision *Fair Housing Council of San Fernando Valley* c. *Roommate.com*[292], la Cour a établi que *Roommate* se qualifiait de fournisseur de contenus[293], en estimant qu'il pose des actes qui sont de nature à structurer, en partie ou en totalité, le contenu de l'information provenant de ses membres[294]. Elle a ensuite conclu qu'il ne pouvait par conséquent se prévaloir de l'immunité prévue par la loi. Toutefois, il faut préciser que cette décision ne représente pas le courant majoritaire américain qui ne tient généralement pas compte du type de structure choisi par le maître du site pour arriver à le qualifier d'hébergeur. Les tribunaux ont jugé que les sites d'agences matrimoniales virtuelles[295] et de vente aux enchères en ligne[296] agissaient en tant que fournisseurs d'hébergement. Ainsi, dans l'affaire *Carafano*[297], la Cour a jugé que *Matchmaker* se qualifiait de fournisseur d'hébergement sur le motif que le contenu du profil émanait uniquement de l'utilisateur qui pouvait, à sa guise, remplir le questionnaire à choix multiples. Par conséquent, la Cour a conclu que *« Matchmaker ne pouvait être tenu responsable, de l'association de certaines réponses à choix multiples avec un ensemble de caractéristiques physiques et une photographie »*.

La tendance générale de la jurisprudence américaine est à l'effet que les blogueurs agissant à titre d'utilisateur d'un service informatique interactif sont également visés par cette exonération de responsabilité. À cet égard, dans un arrêt

---

[292] LLC, *précitée*, note 145. Dans cette décision, l'opérateur du site Roommate.com qui se propose d'offrir à ses membres des services de colocation à l'aide d'outils techniques permettant la création de profils personnels a été poursuivi par avoir contrevenu aux lois relatives à la discrimination en matière de logement. La Cour a établi que pour se qualifier à ce titre, il ne devait jouer aucun rôle actif quant au contenu de l'information à être publiée par le biais de son serveur.

[293] La Cour s'exprime comme suit : « A content provider is « any person or entity that is responsible, *in whole or in part*, for the creation or development of information provided through the Internet." 47 U.S.C. § 230(f)(3).

[294] Si à l'inverse, l'opérateur du site Roommate.com, ne faisait que publier passivement l'information qu'il reçoit de ses membres, il serait alors considéré comme un simple fournisseur d'hébergement et serait visé par cette immunité : *Fair Housing Council of San Fernando Valley* c. *Roommate.com*, LLC, *précitée*, note 145. Voir également *Batzel* c. *Smith*, *précitée*, note 147.

[295] *Carafano* c. *Metrosplash.com Inc.*, *préciée*, note 129 ; Forum des droits sur l'Internet, « États-Unis: extension du régime de responsabilité allégée aux agences matrimoniales virtuelles », *loc. cit*, note 148. Voir également *Batzel* c. *Smith*, *précitée*, note 147, pour la responsabilité imputable à l'administrateur d'une liste de discussion.

[296] *Gentry v. eBay, Inc.*, 99 Cal. App. 4th 816, 830 (2002) ; *Schneider v. Amazon.com, Inc.*, 31 P.3d 37, 39 (Wash.Ct.App. 2001) ; Forum des droits sur l'Internet, « États-Unis : eBay déclaré non responsable des commentaires publiés par les internautes », en ligne sur : < http://www.foruminternet.org/specialistes/veille-juridique/actualites/tats-unis-ebay-declare-non-responsable-des-commentaires-publies-par-les-internautes.html > (visité le 16 février 2009).

[297] *Carafano* c. *Metrosplash.com Inc.*, *précitée*. note 129. L'opérateur du site *Matchmaker.com* qui offre un service de rencontre matrimonial à ses membres est poursuivi sur la base d'atteinte à la vie privée. Les membres peuvent y créer leur propre profil à l'aide d'un questionnaire. Forum des droits sur l'Internet, « États-Unis: extension du régime de responsabilité allégée aux agences matrimoniales virtuelles », *loc. cit*, note 148.

américain[298], la Cour a fixé les conditions d'application de l'immunité prévue à l'article 230(c)(1) de la loi : i) le défendeur doit être un fournisseur de services internet (ISP) ou un utilisateur d'un service informatique interactif ('interactive computer service'); ii) les gestes reprochés au défendeur le sont au regard de ses fonctions d'éditeur (publisher) ou à titre de locuteur (speaker of information) et iii) le message contesté doit être de l'information fournie par un tiers. Le blogueur étant un utilisateur d'un service informatique interactif, il est alors visé par le champ d'application de cette disposition. Rappelons que le maître du blogue est considéré comme un fournisseur de contenus pour ce qui est des contenus qu'il publie lui-même volontairement et un fournisseur d'hébergement pour les fils de discussion figurant à la suite des articles[299]. À cet égard, l'auteure Melissa A. Troiano est d'avis que si la tendance consistant à accorder une large immunité aux utilisateurs d'un service informatique interactif se maintient, les blogueurs auront même le droit de publier des messages à contenu diffamatoire et émanant d'une tierce partie sur leurs sites et ce, en toute impunité[300].

En résumé, l'on a vu que la notion de contrôle ressort du libellé de l'article 230 de *Communication Decency Act* qui offre aux fournisseurs d'accès Internet, aux hébergeurs et aux blogueurs la possibilité de contrôler les contenus circulant via leurs services sans se soucier de voir leur responsabilité civile ou pénale engagée. L'on a observé une certaine tendance dans la jurisprudence américaine à qualifier de fournisseur de contenus le maître du site qui joue un rôle structurant dans la mise en présentation de son site Web. La tendance actuelle démontre une certaine difficulté à établir une distinction claire des notions de fournisseur d'hébergement et de fournisseur de contenus. Rappelons que cette hésitation jurisprudentielle était également présente dans la jurisprudence française. Parallèlement à la *Directive sur le commerce électronique* et la loi française et contrairement à la loi québécoise, la loi

---

[298] *Batzel* c. *Smith, précitée*, note 147.

[299] Lionel THOUMYRE, « La responsabilité pénale et extracontractuelle des acteurs de l'Internet », *loc. cit.*, note 169.

[300] L'auteure dont l'opinion est minoritaire considère que l'application jurisprudentielle de cette disposition a donné lieu à des anomalies à l'endroit des blogueurs. Elle formule le commentaire dans ces mots: « *If the trend toward affording broad immunity to Internet users continues, bloggers will have the ability to post even malicious third-party messages on their sites with impunity.* ». Afin de remédier à la situation, elle formule des recommandations pour que le Congrès apporte des modifications à la présente disposition: « this Comment suggests an amendment to the *CDA* that will hold bloggers who maintain sites that serve the journalistic function of sharing news with the public to the same standard of liability for third-party postings as traditional media defendants »: Melissa A. TROIANO, « Comments –The New Journalism? Why the Traditional Defamation Laws Should Apply to Internet Blogs? », *loc. cit*, note 288.

américaine ne prévoit aucune disposition spécifiquement applicable à l'endroit de l'intermédiaire offrant des services de référence à des documents technologiques.

En conclusion, le législateur américain se montre innovateur en créant le concept d'utilisateurs d'un service informatique interactif. Il adopte une approche qui favorise davantage les utilisateurs d'un service informatique interactif en permettant à ces types d'intermédiaires de retirer ce qui leur *apparaît* comme étant illicite. Cette conception se concilie très mal avec celle des législateurs français, québécois et européen qui, quant à elle, assure une plus grande protection en faveur des tiers. Par conséquent, le droit américain consacre le principe de contrôle comme un critère d'imputabilité applicable aux intermédiaires techniques qu'il qualifie d'utilisateurs d'un service informatique interactif.

Après avoir examiné la notion de contrôle à travers plusieurs législations nationales et internationales, il est possible de dégager plusieurs points qui sont en commun. Premièrement, l'on observe que la notion de contrôle est comprise comme un pré-requis à l'imputation de responsabilité des intermédiaires techniques. Deuxièmement, l'on constate que cette notion peut prendre la forme d'un contrôle physique ou d'un contrôle du sens. L'on voit que la forme de contrôle exercée par l'intermédiaire est modulée selon le type d'actes posés par chacun. Lorsque le geste posé, qu'il soit passif ou actif, affecte le contenu de l'information, l'intermédiaire exerce un contrôle du sens sur l'information. Alors que lorsque l'acte se rattache à un pouvoir de retirer l'information ou d'en empêcher l'accès afin de faire cesser la commission de toute activité illicite, il s'agit d'un contrôle physique. Enfin, l'on a observé que le fait pour l'intermédiaire de poser un geste qui se rattache à un contrôle physique ou à un contrôle du sens est générateur de responsabilité pour ce dernier.

Voyons maintenant comment s'articule la notion de connaissance du caractère illicite du contenu dans ces mêmes lois.

Section II- La connaissance du caractère illicite du contenu

Dans cette section, il convient d'étudier la notion de connaissance, à partir de comparaisons se dégageant de plusieurs législations. Afin d'imputer une responsabilité aux intermédiaires techniques, il importe également d'examiner dans quelle mesure ils ont eu connaissance du caractère illicite de l'information transmise. Pour ce faire,

l'examen de ce critère doit se faire sous l'angle de plusieurs facteurs susceptibles de déterminer la responsabilité imputable à chacun. La question de connaissance de l'information diffusée ne se pose qu'à l'endroit des intermédiaires techniques puisqu'ils ne sont pas assujettis à la présomption de connaissance qui est inhérente à l'exercice de la liberté éditoriale. Lorsque l'acteur disposant de la liberté éditoriale décide de publier de l'information à contenu dommageable, il doit répondre de la responsabilité qui en découle, considérant que la publication d'une telle information suppose une connaissance de première main à l'existence de l'information transmise[301].

Pour que la responsabilité de l'intermédiaire puisse être engagée, il faut notamment démontrer que l'intermédiaire en question avait connaissance de la teneur de l'information transmise par le biais de ses installations[302]. Les circonstances entourant l'imputation de responsabilité des intermédiaires techniques peuvent être décrites comme suit : « *La connaissance, ou l'imputation de la connaissance, peut être établie si l'intermédiaire a exercé un contrôle du contenu des messages diffusés sur le réseau (par exemple, le modérateur d'un tableau d'affichage en ligne, qui filtre les messages avant de les envoyer) ou en cas de circonstances particulières, par exemple si l'opérateur savait que l'utilisateur transmettait de façon répétée des messages diffamatoires et s'il savait qu'un message pouvait être diffamatoire. Cette circonstance particulière peut survenir même dans le cas où un intermédiaire qui n'exerce pas par ailleurs de contrôle du contenu de l'information reçoit des plaintes concernant un émetteur de messages.* »[303].

La connaissance est une condition d'ouverture de la responsabilité des intermédiaires techniques. Dans ce contexte, l'on peut se demander quelle est la portée du critère de connaissance qui sera attribuable à l'intermédiaire technique pour voir sa responsabilité engagée. Quelle est la durée pendant laquelle il doit procéder à l'évaluation de la légalité de l'information? D'autre part, qu'en est-il de la valeur du contenu du message véhiculé? Quels critères doit-il utiliser afin de déterminer si tel message est susceptible de causer des dommages à des tiers?

---

[301] L.E. BECKER Jr., « The Liability of Computer Bulletin Board Operators for Defamation Posted by Others », *loc. cit.*, note 88, p. 203, 217; Pierre TRUDEL « Les responsabilités dans le cyberspace », *supra*, note 91, p. 242.
[302] Pierre TRUDEL, « Les responsabilités dans le cyberespace », *supra*, note 33, p. 254.
[303] Henry H. PERRITT Jr., « Tort liability, the first amendment and equal access to electronic networks », *loc. cit.*, note 209, p. 65, 107.

Dans l'affaire *Religious Technology Center* v. *Netcom Online Communication Services Inc.*[304], la Cour s'est prononcée sur ces questions, notamment sur la portée des obligations mises à la charge des intermédiaires techniques après la connaissance de l'information dommageable. En l'espèce, un ancien adepte de l'Église de Scientologie avait diffusé, par le biais du forum de discussion, des informations concernant le fondateur de cette organisation, en violation de ses droits et de celle de l'éditeur. Une fois mise au courant de la violation, ils ont poursuivi entre autres le fournisseur d'accès Internet. La Cour énonce que la seule responsabilité pouvant lui être imputable est la « *complicité de contrefaçon* »[305] en précisant les conditions qui y donnent ouverture, soit a) la connaissance de l'activité illicite et b) une participation substantielle à celle-ci. Or, l'Église de Scientologie avait demandé la cessation immédiate de la contrefaçon par le biais de ses services à l'opérateur du système qui aurait refusé d'y acquiescer en exigeant des preuves supplémentaires à l'appui de ses prétentions. De ce fait, elle se retrouvait à remplir la condition de connaissance de l'infraction et ne pouvait, par conséquent, invoquer la défense de « *fair use* »[306] afin de s'exonérer de sa responsabilité. De plus, la Cour a établi que *Netcom* doit être tenu responsable de son inaction, ce qui sera assimilé à une participation substantielle dans la distribution illégale du matériel[307]. En l'espèce, la preuve soumise est à l'effet que *Netcom* n'avait pas jugé utile de procéder à l'examen de la légalité du matériel en question, même s'il s'avérait « *potentiellement* » illégal[308]. En ce sens, la Cour a tort d'assimiler l'inaction de l'opérateur du système à une faute, considérant que la faute suppose l'existence d'un réel manquement à la loi. Or, à la lumière des faits, il n'y avait aucune preuve démontrant une contravention manifeste à la loi. Il faut préciser que, selon sa

---

[304] 907 F. Supp. 1361 (N.D. Cal.1995).

[305] *Religious Technology Center* v. *Netcom Online Communication Services Inc.*, *précitée*, note 304. La Cour précise que Netcom ne peut être tenu responsable d'une « contrefaçon directe » dans la mesure où il n'a pas personnellement diffusé le matériel illégal.

[306] Le « *fair use* » désigne le droit d'utiliser une création sans enfreindre le droit de la propriété intellectuelle. Ce concept se retrouve dans la loi américaine sur le copyright : Legalis.net, « Commentaire de l'ordonnance rendue par la "Northern District Court of California", le 21 novembre 1995, *Religious Technology Center (Eglise de Scientologie)* c./ *Netcom*, –Responsabilité d'un prestataire de services en ligne et de son fournisseur d'accès, en matière de contrefaçon commise par un abonné du prestataire », en ligne sur : < http://www.legalis.net/cgi-iddn/french/affiche-jnet.cgi?droite=commentaires/comm_netcom_1195.htm > (visité le 28 juin 2007) ; *Religious Technology Center* v. *Netcom Online Communication Services Inc.*, *précitée*, note 304.

[307] *Religious Technology Center* v. *Netcom Online Communication Services Inc.*, *précitée*, note 304 ; Pierre TRUDEL, « Les responsabilités dans le cyberespace », *supra*, note 91, p. 254.

[308] *Religious Technology Center* v. *Netcom Online Communication Services Inc.*, *précitée*, note 304 ; Pierre TRUDEL, « Les responsabilités dans le cyberespace », *supra*, note 91, p. 254.

perception de la situation, l'opérateur du système croyait sincèrement qu'il n'avait aucune obligation d'agir, vu que la preuve n'établissait pas suffisamment l'illégalité du matériel. Par conséquent, cette décision comporte une réelle difficulté de déterminer le poids à donner au concept de notification permettant de produire une obligation d'agir à l'encontre de l'intermédiaire. Le juge et l'intervenant donnent des interprétations différentes au rôle que doit assumer l'intermédiaire dans la prévention des dommages pouvant être causés à des tiers : l'un voit là une obligation *a priori* et l'autre *a posteriori*[309].

Toutefois, l'approche qui consiste à n'imposer aucune obligation à l'encontre des intermédiaires techniques jusqu'attend qu'un jugement tranche sur le caractère dommageable de l'information n'est également pas envisageable. En effet, l'auteur Henry H. Perritt Jr. est d'avis qu'une telle approche risquerait de « *créer un préjudice substantiel irréparable aux titulaires de droits d'auteur* »[310]. Par conséquent, il faut concevoir qu'il doit tout de même exister une certaine obligation de prévention des dommages qui peuvent s'ensuivre[311].

Si l'obligation d'agir existe dès lors qu'il y a une « *possibilité* » de causer des dommages à autrui, il faut se demander si on n'en vient pas à lui incomber un rôle allant au-delà de sa qualité de simple « intermédiaire ». Lorsqu'un intervenant publie de l'information, il est au courant du caractère potentiellement préjudiciable du matériel transmis à l'égard des tiers, c'est pourquoi il est tout à fait justifié de lui imputer une obligation de compétence à l'égard de l'information qu'il a la faculté de corriger alors que dans le cas d'un intermédiaire qui n'est pas impliqué dans la production de l'information, il est difficile de voir comment peut-on lui imputer une telle obligation, étant donné qu'il peut difficilement savoir que celle-ci est susceptible de causer un dommage à autrui[312]. Par conséquent, il est préférable d'imposer une obligation de prévention qui serait limitée aux cas où il peut « raisonnablement » agir.

---

[309] Le juge interprète la notion de notification plus restrictivement, en exigeant de l'intermédiaire d'agir à partir du moment où il y a une « possibilité » d'atteinte aux droits des tiers alors que l'intermédiaire lui donne une interprétation large, en exigeant qu'on lui fournisse des preuves établissant *prima facie* la violation du droit. Il faut mentionner que les intermédiaires techniques n'ont généralement pas comme politique d'exercer un contrôle éditorial sur l'information : Pierre TRUDEL, « Les responsabilités dans le cyberespace », *supra*, note 91, p. 254.

[310] Henry H. PERRITT Jr., « Computer crimes and torts in the global information infrastructure : intermediaires and jurisdiction », 12 octobre 1995.

[311] À titre d'exemple, voir les articles 12(3), 13(2) et 14(3) de la *Directive sur le commerce électronique*.

[312] J.H. SPOOR, « Database Liability : Some General Remarks », (avril 1989) 3 *International Computer Law Adviser* 4, p. 6.

Dans cette perspective, il y a lieu d'analyser, dans cette section, l'interprétation du principe de connaissance dans plusieurs législations dont la *Convention sur la cybercriminalité*.

A) La *Convention sur la cybercriminalité*

Dans ce paragraphe, il y a lieu d'étudier les dispositions de la Convention et du Protocole qui traitent du principe de connaissance à l'égard des intermédiaires techniques.

Tout d'abord, l'on débutera notre analyse avec la Convention. Cet instrument juridique organise la notion de connaissance dans une série de dispositions qui ne visent que l'auteur du crime. Seule la disposition visant la complicité[313] se trouve directement applicable aux intermédiaires techniques puisque ces derniers, tout comme le complice, jouent un rôle secondaire dans la commission d'une infraction. Cette disposition met toutefois sur le même pied d'égalité tous les intermédiaires techniques puisqu'il n'établit pas de réelles distinctions à l'égard de chacun d'eux.

Aux termes du premier paragraphe de la disposition visant la complicité[314], la responsabilité de l'intermédiaire qui aide l'auteur du crime à commettre l'une des infractions établies par la Convention[315] ne peut être engagée que s'il a l'intention qu'une telle infraction soit commise. L'intermédiaire ne peut alors être tenu responsable que s'il a l'intention criminelle requise. À cet égard, le rapport explicatif fait un rapprochement entre l'intention et la connaissance en mentionnant ce qui suit : « *[a]insi, par exemple, la responsabilité peut être imposée s'il y a "connaissance et contrôle" de l'information transmise ou stockée. Il ne suffit pas, par exemple, qu'un fournisseur de services serve d'intermédiaire pour la transmission de ce matériel, par le biais d'un site Web ou d'un bavardoir, entre autres moyens, en l'absence de l'intention requise en l'occurrence en droit interne* »[316]. Ainsi, l'intention de commettre un acte de complicité implique pour l'intermédiaire d'avoir connaissance du caractère illicite de l'activité commise par

---

[313] La disposition visant la complicité en vue de la perpétration des infractions définies dans la Convention (c'est-à-dire les articles 2 à 10) est incriminée à l'article 11 de la Convention.

[314] L'on retrouve également les infractions de tentative de commettre les infractions définies dans la Convention et la complicité en vue de leur perpétration qui sont prévues à l'article 11 de la Convention.

[315] Ces infractions sont prévues aux articles 2 à 10 de la Convention.

[316] *Convention sur la cybercriminalité*, Rapport explicatif, *loc. cit.*, note 24, par. 105.

l'auteur du crime[317]. En d'autres mots, l'intermédiaire qui a l'intention qu'une infraction soit commise par l'auteur du crime agit en tant que complice, en sachant les conséquences résultant de l'acte en question et en étant insouciant face à ces conséquences. L'on peut donner plusieurs exemples de situations qui se rapportent au concept de connaissance. À titre d'exemple, un intermédiaire technique ne peut être responsable que s'il a l'intention d'aider l'auteur du crime à *offrir*, à *rendre disponible*, à *diffuser*, à *transmettre*, à *produire* ou à *posséder* de la pornographie juvénile[318]. Ce qui suppose pour l'intermédiaire d'être au courant de la nature illicite du contenu concerné su Internet. Comme autre exemple, un fournisseur d'accès Internet qui aide l'auteur du crime à transmettre des données relativement à un contenu nuisible ou à un code malveillant doit avoir l'intention qu'une telle infraction soit commise pour engager sa responsabilité pénale à titre de complice[319]. Ce qui implique une intention malicieuse ou malhonnête de participer à la commission de cette infraction à titre de complice. Comme autre exemple, prenons le cas où l'intermédiaire aide l'auteur du crime à commettre l'infraction liée à l'entrave des données[320]. Ainsi, si cet intermédiaire aide l'auteur du délit à *supprimer*, à *effacer*, à *détériorer* ou à *endommager* des données avec l'intention qu'une telle infraction soit perpétrée, c'est qu'il a un état de conscience qui souhaite la réalisation des actes posés, c'est-à-dire entraver les données du système informatique. Le fait pour cet intermédiaire d'être conscient de la visée criminelle de l'infraction ou d'être mis devant des faits qui rendent possibles la commission de l'infraction suppose la connaissance du caractère illicite de cette activité.

---

[317] L'on verra dans le paragraphe A) du chapitre II du titre II traitant de l'application des principes d'imputabilité des intermédiaires techniques qu'en droit pénal canadien, l'élément mental est formé de deux composantes, à savoir la connaissance et l'intention. La connaissance se présente sous trois formes : la connaissance réelle, l'ignorance volontaire et la connaissance imputée. L'intention, quant à elle, se rapporte soit à l'intention générale, soit à l'intention spécifique. Par conséquent, l'on peut alors faire des rapprochements avec la connaissance puisque les deux concepts se rapportent à l'élément mental d'une infraction.

[318] *Convention sur la cybercriminalité*, Rapport explicatif, *loc. cit.*, note 24, par. 105 ; article 9 de la Convention.

[319] *Convention sur la cybercriminalité*, Rapport explicatif, *loc. cit.*, note 24, par. 119. Pour ce qui est de l'infraction de tentative, la responsabilité n'est engagée que lorsque l'acte de tentative est commis intentionnellement. Comme l'incrimination de l'infraction de tentative est inconcevable pour certaines infractions ou éléments desdites infractions définies dans la Convention, notamment les éléments relatifs au fait d'offrir ou de rendre disponible de la pornographie juvénile, l'on a jugé utile de permettre aux Parties d'incriminer la tentative que dans le cas d'infractions établies en application des dispositions spécifiques : C'est-à-dire les articles 3, 4, 5, 7, 8, 9.1a) et 9.1c) de la Convention : *ibid*, par. 120.

[320] Cette infraction est incriminée à l'article 5 de la Convention.

Contrairement aux autres instruments juridiques nationaux et internationaux qui apportent des nuances entre chacun des intermédiaires quant à l'interprétation du concept de connaissance, la Convention n'établit pas de telles distinctions. Elle se concentre davantage sur les différentes infractions et crée des variations quant au niveau de connaissance requis dans la commission d'une infraction[321]. Puisque la Convention constitue tout d'abord un instrument de répression pénale et ce, contrairement aux autres instruments juridiques nationaux et internationaux.

Dans un deuxième temps, il faut examiner comment s'articule le principe de connaissance dans le Protocole. Tout comme la Convention, le Protocole prévoit différentes dispositions qui ne s'appliquent qu'à l'auteur du crime, à l'exception d'une seule qui se trouve applicable à l'égard de tous les intermédiaires techniques, à savoir celle liée à la complicité[322]. Cette disposition organise un régime de responsabilité qui est commun à tous les intermédiaires techniques, sans relever les différentes nuances pouvant exister entre chacun d'eux.

Le principe de connaissance ressort du premier paragraphe de la disposition visant la complicité[323] qui dispose qu'un intermédiaire ne peut être tenu responsable que s'il a l'intention d'aider l'auteur du crime dans la commission de l'une des infractions du Protocole[324]. À cet égard, le rapport explicatif du Protocole reprend essentiellement les commentaires formulés dans la Convention au sujet du possible rapprochement que l'on peut faire entre l'intention et la connaissance[325]. L'on peut fournir plusieurs cas de figure qui se rapportent à la connaissance. À titre d'exemple, un intermédiaire qui aide l'auteur du crime à transmettre du matériel raciste et xénophobe ne peut engager sa responsabilité pénale que s'il a l'intention que l'auteur

---

[321] Tantôt elle exige une intention générale tantôt une intention spécifique de commettre une infraction. À titre d'exemple, les infractions liées à l'abus de dispositifs, à la falsification informatique, à la fraude informatique exigent l'intention spécifique de commettre une infraction : Ces infractions sont prévues aux articles 6, 7 et 8 de la Convention.

[322] La disposition visant la complicité est incriminée à l'article 7 du Protocole.

[323] En vertu de l'article 7 du Protocole.

[324] *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, Rapport explicatif, *loc. cit.*, note 28, par. 25, 45.

[325] Le rapport explicatif du Protocole mentionne ce qui suit : « Une personne ne peut être responsable pour une quelconque infraction contenue dans ce Protocole si elle n'a pas agi avec intention délictueuse. Il ne suffit pas, par exemple, pour que la responsabilité pénale d'un fournisseur de services soit engagée, que ce dernier sert d'intermédiaire pour la transmission de ce type de matériel par le biais d'un site Web ou d'un bavardoir, en l'absence de l'intention requise en droit interne dans le cas particulier » : *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, Rapport explicatif, *loc. cit.*, note 28, par. 25.

du crime procède à la commission d'une telle infraction[326]. Ce qui implique la connaissance du caractère illicite de l'activité en question. Comme autre exemple, le fait pour l'intermédiaire d'aider l'auteur du délit à disséminer du matériel raciste et xénophobe à autrui, à l'échanger sur un forum de discussion ou à en faire la distribution[327] avec l'intention qu'une telle infraction soit commise implique pour ce dernier la connaissance du caractère illicite de cette activité. Comme autre exemple, un intermédiaire qui aide l'auteur du crime à accéder à un service de vente aux enchères à des fins d'exposition d'objets nazis peut être tenu responsable à titre de complice s'il a l'intention qu'une telle infraction[328] soit commise. Ainsi, comme il permet l'accès à un service de vente d'objets nazis, sachant que ce service constitue une fin illégale, l'on présume qu'il a l'intention que la nature illicite du contenu soit mise à la disposition du public par le biais d'un système informatique, ce qui suppose la connaissance du caractère illégal de cette activité.

Alors que les autres instruments juridiques établissent un même degré de connaissance à l'égard de tous les intermédiaires, le Protocole apporte des variations quant au degré de connaissance requis dans la commission d'une infraction[329]. Puisque le Protocole, contrairement aux autres instruments juridiques, constitue un instrument de répression pénale.

Après avoir analysé la notion de connaissance dans la Convention et le Protocole, l'on peut alors faire les constats suivants. Premièrement, seules les dispositions qui visent la complicité s'appliquent directement aux intermédiaires techniques[330]. Ces dispositions traitent du principe de connaissance de la même manière à l'égard de tous les intermédiaires techniques. Deuxièmement, ces deux

---

[326] *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, Rapport explicatif, *loc. cit.*, note 28, par. 45.

[327] Il s'agit d'infractions relatives à la diffusion de matériel raciste et xénophobe qui sont incriminées à l'article 3 de la Convention. Cette disposition prohibe la diffusion et de toutes autres formes de mise à disposition du public, par le biais du système informatique, de matériel raciste ou xénophobe.

[328] L'infraction qui est relative à la négation, à la minimisation de façon grossière, à l'approbation ou à la justification du génocide est prévue à l'article 6 du Protocole. Plus précisément, l'on incrimine la diffusion ou les autres formes de mise à disposition du public, par le biais d'un système informatique, de matériel qui nie, minimise de manière grossière, approuve ou justifie de façon intentionnelle et sans droit les actes qui relèvent de génocide ou de crimes contre l'humanité, tels que définis par le droit international et reconnus comme tels par une décision finale et définitive du Tribunal militaire international ou par tout autre tribunal international établi par des instruments juridiques internationaux pertinents : art. 6 du Protocole.

[329] Parfois, l'instrument requière l'intention générale de commettre une infraction alors que d'autres fois, il exige une intention spécifique. À titre d'exemple, l'article 6 du Protocole qui incrimine la négation, la minimisation grossière, l'approbation ou la justification du génocide ou des crimes contre l'humanité.

[330] C'est-à-dire l'article 11 de la Convention et l'article 7 du Protocole.

instruments juridiques organisent la notion de connaissance selon un niveau qui peut varier selon qu'il s'agit d'une intention générale ou d'une intention spécifique.

En conclusion, le principe de connaissance s'exprime par le concept de l'intention et demeure enraciné dans le texte de la Convention et du Protocole comme élément constitutif de l'infraction, c'est-à-dire un pré-requis à l'imputation de la responsabilité des intermédiaires techniques.

Examinons maintenant le principe de connaissance dans la *Directive sur le commerce électronique.*

B) La *Directive sur le commerce électronique*

Dans cette section, il convient d'étudier les principales dispositions de la *Directive sur le commerce électronique* qui appliquent la notion de connaissance à l'égard des intermédiaires techniques[331]. Le texte européen applique spécifiquement le principe de connaissance à l'égard des seuls intermédiaires suivants : le transmetteur, l'intermédiaire assurant une activité de stockage automatique dans le seul but de rendre plus efficace la transmission ultérieure de l'information et l'hébergeur.

Tout d'abord, il faut étudier la disposition qui traite de la notion de connaissance à l'égard du transmetteur[332]. Contrairement aux dispositions qui concernent le prestataire assurant une activité de stockage automatique dans le seul but de rendre plus efficace la transmission ultérieure de l'information et l'hébergeur, celle qui vise le transmetteur n'énonce pas expressément la notion de connaissance et ce, parallèlement aux lois québécoise et française[333]. Toutefois, l'absence de texte spécifique prévoyant le principe de connaissance applicable à l'égard du transmetteur ne signifie pas que ce principe ne s'applique aucunement à cet intermédiaire. Puisque ce principe découle implicitement du libellé de l'article 12 de la *Directive sur le commerce électronique* qui prévoit que le transmetteur peut engager sa responsabilité dans trois cas précis, à savoir être à l'origine de la transmission, sélectionner le

---

[331] Voir, *supra*, note 15. Il s'agit des articles 12, 13 et 14 de la *Directive sur le commerce électronique.* Contrairement à la *Convention sur la cybercriminalité* et parallèlement aux lois québécoise et française, la *Directive sur le commerce électronique* s'attache à préciser le cadre juridique applicable à chacun des intermédiaires en fonction du rôle qu'il assume dans la chaîne de communication.

[332] En vertu de l'article 12 de la *Directive sur le commerce électronique.*

[333] Voir l'article 36 de la *LCCJTI* et l'article 9 de la loi française qui réfère à l'article L. 32-3-3 du *Code des postes et des communications électroniques.*

destinataire de la transmission et sélectionner et modifier les informations faisant l'objet de la transmission. Ces trois situations impliquent que le transmetteur puisse être au courant du caractère illicite de l'information ou activité en question ou qu'il soit mis devant des faits qui rendent apparente la présence de ces activités ou informations. Puisque être à l'origine de l'information signifie que l'intermédiaire désire transmettre l'information en question, sachant qu'elle comporte des contenus illicites. Sélectionner de la transmission suppose que l'intermédiaire connaisse la personne à qui il désire envoyer le contenu litigieux et modifier le contenu de l'information implique une connaissance réelle du contenu véhiculé par le transmetteur. Contrairement aux autres instruments juridiques qui énoncent explicitement le principe de connaissance à l'égard du transmetteur, le législateur européen préconise une rédaction qui présente implicitement ce principe à l'égard de cet intermédiaire.

En deuxième lieu, il faut examiner la disposition qui traite de la notion de connaissance à l'égard de l'intermédiaire qui assure une activité de stockage automatique dans la seule fin de rendre plus efficace la transmission ultérieure de l'information[334]. Il faut souligner que, contrairement à la disposition concernant le transmetteur, cette disposition, tout comme celle qui vise l'hébergeur, énonce explicitement la notion de connaissance. Suivant l'article 13 de la *Directive sur le commerce électronique*, dès que le prestataire en question a *effectivement connaissance* i) du fait que l'information à l'origine de la transmission a été retirée du réseau ou ii) du fait que l'accès à l'information a été rendu impossible ou iii) du fait qu'un tribunal ou une autorité administrative a ordonné de retirer l'information ou d'en rendre l'accès impossible, il doit agir avec promptitude pour retirer l'information litigieuse ou pour en rendre l'accès impossible. Aux termes de cette disposition, l'intermédiaire peut avoir *effectivement connaissance* dans trois cas précis : i) lorsque l'information émane de lui-même ou qu'il est la personne qui a pris la décision de la diffuser ; ii) lorsque ce dernier effectue une surveillance sur l'information et qu'il a rendu l'accès impossible à celle-ci ou iii) lorsqu'il a obtenu confirmation par une autorité indépendante du caractère illicite de l'information. Le fait d'avoir *effectivement connaissance* de l'activité ou information litigieuse se rattache à une connaissance réelle. Celle-ci peut

[334] En vertu de l'article 13 de la *Directive sur le commerce électronique*.

être obtenue à la suite de la réception d'une plainte par une tierce partie. Dans ce contexte, se pose la question de savoir si la réception d'une simple plainte équivaut à une *connaissance effective* de l'illicéité de l'information en question. À ce sujet, l'auteur Trudel formule les commentaires suivants : « *[l]a connaissance à partir de laquelle est engendrée la responsabilité n'est pas celle qui résulte de la seule réception d'une plainte mais vise plutôt le moment où le caractère illicite devient manifeste. C'est ce qui permet de dire que lorsque le caractère illicite est, à sa face-même, manifeste, la connaissance est acquise dès le moment où l'on apprend son existence* »[335]. Ainsi, la simple réception d'une plainte par un tiers n'obligerait pas cet intermédiaire à retirer le contenu litigieux si une autorité indépendante ne confirmerait pas le caractère sérieux de la plainte. Par ailleurs, les législateurs québécois et français adoptent une même attitude en prévoyant expressément le principe de connaissance à l'égard de cet intermédiaire[336]. Il est possible d'apporter une nuance quant aux choix de termes employés dans la loi québécoise. Ainsi, le législateur québécois[337] réfère à une connaissance « *de fait* » alors que les législateurs français et européen se rapportent à une connaissance « *effective* »[338] dans la disposition qui traite du principe de connaissance à l'égard de cet intermédiaire pour chacune de ces législations. Cette légère nuance importe peu puisque tous les législateurs réfèrent à la procédure de notification, même si le législateur ne l'exprime pas directement. Malgré cette différence terminologique, tous les textes se concordent globalement sur le principe de connaissance. Toutefois, la *Convention sur la cybercriminalité* qui ne se rallie pas aux autres instruments juridiques comprend ce principe d'une manière restrictive pour les infractions relatives à l'abus de dispositifs, à la falsification informatique, à la fraude informatique et celle relative à la répression de crimes visant à nier, minimiser de façon grossière, approuver

---

[335] Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit.*, note 47, p. 21.

[336] En vertu de l'article 37 de la *LCCJTI* et l'article 9 de la loi française qui réfère à l'article L. 32-3-4 du Code des postes et des communications électroniques

[337] En vertu de l'article 37 de la *LCCJTI* qui énonce ce qui suit : [...] Il peut engager sa responsabilité, notamment s'il participe autrement à l'action d'autrui : [...]4°en ne retirant pas promptement du réseau ou en ne rendant pas l'accès au document impossible alors qu'il a de fait connaissance qu'un tel document a été retiré de là où il se trouvait initialement sur le réseau, du fait qu'il n'est pas possible aux personnes qui y ont droit d'y avoir accès ou du fait qu'une autorité compétente en a ordonné le retrait du réseau ou en a interdit l'accès.

[338] En vertu de l'article 9 de la loi française référant à l'article L. 32-3-4 du *Code des postes et des communications électroniques* qui énonce ce qui suit : [...] 2° Elle n'a pas agi avec promptitude pour retirer les contenus qu'elle a stockés ou pour en rendre l'accès impossible, dès qu'elle a effectivement eu connaissance, soit du fait que les contenus transmis initialement ont été retirés du réseau, soit du fait que l'accès aux contenus transmis initialement a été rendu impossible, soit du fait que les autorités judiciaires ont ordonné de retirer du réseau les contenus transmis initialement ou d'en rendre l'accès impossible. .

ou justifier le génocide. Puisque l'élément intentionnel spécifique supplémentaire est requis comme partie intégrante de l'infraction. Cela se comprend puisque la Convention constitue tout d'abord un instrument de répression pénale, alors il est normal qu'elle soit à portée restrictive. Par conséquent, la *Convention sur la cybercriminalité* est le texte qui interprète le plus restrictivement le principe de connaissance.

En troisième lieu, il y a lieu de faire état de la disposition qui applique la notion de connaissance à l'égard de l'hébergeur[339]. L'article 14 de la *Directive sur le commerce électronique* De cette disposition se dégagent deux variantes de la notion de connaissance. D'une part, la connaissance réelle qui peut provenir soit de lui-même, soit d'une tierce partie[340] par laquelle l'hébergeur est mis au courant de l'illicéité de l'information ou activité en question. Il est à préciser que les commentaires formulés plus haut en ce qui concerne l'intermédiaire assurant une activité de stockage automatique afin de rendre plus efficace la transmission ultérieure de l'information s'applique également à l'égard de cet intermédiaire[341]. D'autre part, la connaissance qui découle d'un ensemble de circonstances qui rendent apparentes la réalisation de l'activité illicite. À l'exception des cas clairs d'illicéité, au nom de quelle autorité devrait-il s'ériger en juge afin de déterminer le caractère illicite de telle ou telle information? Le fait pour le législateur européen d'inclure également l'apparence d'illicéité de l'activité ou de l'information en question dans le libellé de la disposition manifeste son intention d'appliquer une interprétation plus large du principe de connaissance à l'égard de cet intermédiaire alors qu'il se montre plus rigoureux à l'égard des deux autres intermédiaires en prévoyant que la responsabilité serait engagée dans le seul cas où l'intermédiaire en question aurait *effectivement* connaissance des activités ou informations illicites[342]. Le législateur européen souhaite viser plus de situations pouvant relever du caractère illicite de l'activité ou information

---

[339] Article 14 de la *Directive sur le commerce électronique.*

[340] Par exemple, les procédures de notification et de retrait, telles que l'on retrouve dans le *Digital Millenium Copyright Act.* Il faut préciser que cette procédure n'est pas couverte par la *Directive sur le commerce électronique* qui laisse le loisir aux Parties de les mettre en place et mentionne dans son article 22 mentionne la nécessité de présenter des propositions relatives aux procédures de notification et de retrait

[341] Voir *supra*, p. 80-81.

[342] Outre bien sûr le fait que l'accès à l'information a été rendu impossible, ou le fait qu'un tribunal ou une autorité administrative a ordonné de retirer l'information ou d'en rendre l'accès impossible : article 14 de la *Directive sur le commerce électronique.*

en question. Les législateurs québécois et français suggèrent une formulation identique au législateur européen [343]. Toutefois, à la différence de la *Directive sur le commerce électronique*, la *Convention sur la cybercriminalité* et la loi américaine ne prévoient pas textuellement le principe de connaissance directement applicable à l'hébergeur, c'est par l'interprétation de chaque infraction et mesure que l'on peut en déduire. En outre, l'article 14 de la *Directive sur le commerce électronique* impose une obligation *a posteriori* à l'encontre de l'hébergeur qui est mis au courant du caractère illicite de l'activité ou information en question. Ainsi, cette disposition énonce que cet intermédiaire doit agir promptement *pour retirer* le contenu litigieux ou *en rendre l'accès impossible où il en a eu connaissance*. Cette obligation d'agir se présente également dans le texte français avec une pareille formulation[344] alors que la *Convention sur la cybercriminalité* reste muette à ce sujet. Contrairement à la *Directive sur le commerce électronique*, la loi française érige expressément une responsabilité pénale à l'égard de l'hébergeur qui omet de retirer le contenu litigieux ou de faire cesser l'activité illicite[345].

En résumé, la *Directive sur le commerce électronique* organise un cadre juridique qui prévoit le principe de connaissance à l'égard du transmetteur, de l'intermédiaire assurant une activité de stockage automatique dans le seul but de rendre plus efficace la transmission ultérieure de l'information et de l'hébergeur. L'on a vu qu'elle énonce expressément la notion de connaissance à l'égard de ces intermédiaires techniques, à l'exception du transmetteur. L'on a constaté que le législateur européen adopte une rédaction plus généreuse à l'égard de l'hébergeur en couvrant les faits ou circonstances qui rendent apparentes l'illicéité de l'information ou activité en question. L'on a remarqué que l'articulation du principe de connaissance dans la *Directive sur le commerce électronique* était similaire aux lois française et québécoise mais divergente dans la loi américaine et dans la *Convention sur la cybercriminalité* qui fournit une interprétation restrictive à cette notion. L'on a également dégagé les principales obligations mises à la charge des intermédiaires techniques qui sont déclenchées à partir du moment où ils ont *effectivement connaissance* de l'activité illicite. Avant ce

[343] En vertu de l'article 22(2) de la *LCCJTI* et de l'article 6-I-2 de la *LCEN*.
[344] En vertu de l'article 6-I-2 de la *LCEN*.
[345] En vertu de l'article 6-I-3 de la *LCEN*.

moment, ils ont l'obligation d'agir avec une certaine retenue. Ils doivent s'efforcer d'adopter une conduite qui soit empreinte d'indifférence face à la diffusion du contenu de l'information. Ils ne doivent s'ingérer d'aucune façon dans le cours du traitement des données. À l'inverse, après ce moment, ils doivent agir rapidement de façon à retirer l'information dommageable ou autrement faire cesser la poursuite de l'activité.

En conclusion, l'on peut constater que le principe de connaissance ressort expressément de cet instrument international en tant principe d'imputabilité applicable à l'égard du transmetteur, de l'intermédiaire assurant une activité de stockage automatique dans le seul but de rendre plus efficace la transmission ultérieure de l'information et à l'égard de l'hébergeur.

Après avoir examiné les principales dispositions du texte européen qui traitent de la notion de connaissance, parcourons maintenant celles qui proviennent de la loi française.

C) La *Loi pour la confiance dans l'économie numérique*

Dans cette section, il convient d'étudier la *Loi pour la confiance dans l'économie numérique*[346] (ci-après : « *LCEN* ») qui intègre dans une série de dispositions, y incluant celles du *Code des postes et des communications électroniques*, le principe de connaissance qui est applicable aux intermédiaires techniques. Parallèlement à la *Directive sur le commerce électronique* et à la québécoise, la loi française énonce explicitement le principe de connaissance à l'égard de tous les intermédiaires techniques, en mettant à l'écart le transmetteur. Toutefois, à la différence de la loi française, la *Convention sur la cybercriminalité* se montre beaucoup plus précise quant au niveau de connaissance requis pour chacune des

---

[346] Voir, *supra*, note 16. La *LCEN* s'attache à instaurer un régime de responsabilité devant favoriser le commerce électronique et renforcer la sécurité des transactions en ligne, tout en sachant bien composer avec les droits fondamentaux, la liberté d'expression et la protection de droits individuels. La *LCEN* constitue un régime juridique qui tient compte du respect de la dignité de la personne humaine, de la liberté et de la propriété d'autrui, du caractère pluraliste de l'expression des courants de pensée et d'opinion et de la nécessité d'assurer la sauvegarde de l'ordre public, la protection des mineurs et de la société des activités illicites commises dans le cyberespace. Le cadre juridique qu'elle prétend ainsi mettre sur pied vise à aller vers « *un partage réaliste et équilibré des responsabilités de chacune des parties* » : Le Portail Société de l'Information Internet, « Loi pour la confiance dans l'économie numérique », en ligne sur : < http://www.internet.gouv.fr/information/information/dossiers/loi-pour-confiance-dans-economie-numerique-len/adoption-loi-pour-confiance-dans-economie-numerique-len-40.html > (visité le 20 juillet 2007). La *LCEN* propose une responsabilité qui est limitée à certaines conditions qui une fois remplies, exonèrent le prestataire en question.

infractions répertoriées mais a le désavantage d'appliquer le principe de connaissance uniformément à l'égard de tous les intermédiaires techniques. Dans ce contexte, examinons comment le principe de connaissance est compris dans chacune des dispositions visant successivement l'hébergeur, le transmetteur et l'intermédiaire assurant une activité de stockage automatique dans le seul but de rendre plus efficace la transmission ultérieure de l'information.

En premier lieu, débutons notre étude avec la disposition visant l'hébergeur[347]. Contrairement à la *Directive sur le commerce électronique*, la loi française institue un régime de responsabilité qui s'applique tant au niveau civil que pénal. Aux termes de l'article 6-1-2 de la *LCEN*, la responsabilité civile de l'hébergeur peut notamment être engagée i) *s'il a effectivement connaissance du caractère illicite de l'information ou des activités ou* ii) *des faits et circonstances faisant apparaître ce caractère.* Aux termes de l'article 6-I-3 de la *LCEN*, la responsabilité pénale de l'hébergeur peut notamment être emportée s'il a *effectivement connaissance de l'activité ou de l'information illicites.* La rédaction des deux alinéas est sensiblement la même, à la différence que la connaissance découlant de *l'apparence d'illicéité* n'est pas retranscrite dans l'alinéa visant la responsabilité pénale de cet intermédiaire. Cette omission est liée au fait que cet alinéa doit faire l'objet d'une interprétation restrictive en raison de la nature pénale de son champ d'application. La rédaction de la *LCEN* se concilie bien avec la *Directive sur le commerce électronique* qui comprend également la notion de *l'apparence d'illicéité* à l'égard de l'hébergeur[348]. La connaissance du caractère illicite des informations ou activités peut résulter soit d'une *connaissance effective*, soit *d'un ensemble de faits rendant apparent ce caractère.*

Premièrement, la *connaissance effective* peut émaner de l'hébergeur lui-même, notamment lorsqu'il décide de publier ou de modifier l'information litigieuse ou d'effectuer une surveillance sur l'activité en question. La *connaissance effective* peut également être acquise à la suite d'une notification par une tierce partie. À cet égard, contrairement à la *Directive sur le commerce électronique*, la *LCEN* institue un mécanisme de notification de l'hébergeur[349]. Aux termes de cette disposition, la

---

[347] En vertu des articles 6-I-2 et 6-I-3 de la *LCEN*.
[348] En vertu de l'article 14 de la *Directive sur le commerce électronique*.
[349] Par le biais de son article 6-I-5 de la *LCEN*.

connaissance des faits litigieux est présumée acquise par cet intermédiaire dès lors qu'un certain nombre d'informations lui est notifié, notamment « *la description des faits litigieux et leur localisation précise* » ainsi que les « *motifs [de droit] pour lesquels le contenu doit être retiré*».[350]. À cet égard, les tribunaux[351] ont condamné les demandeurs pour ne pas avoir eu recours à cette procédure de notification ou pour ne pas avoir respecté le formalisme édicté par la loi[352]. Par ailleurs, l'article 6-I-4 sanctionne « *d'une peine d'un an d'emprisonnement et de 15 000 € d'amende* » les cas de dénonciations abusives[353]. À la différence de la *Directive sur le commerce électronique* et de la loi québécoise, il faut constater que la loi française prévoit explicitement des mesures de sanctions pénales. Le législateur responsabilise alors le dénonciateur de contenus illicites[354].Contrairement à la loi française, la *Directive sur le commerce électronique* et la *Convention sur la cybercriminalité* ne comportent pas de telle procédure de notification. Ainsi, la *LCEN* met en place des conditions de forme permettant d'une part, de vérifier de la légalité procédurale de la notification et d'autre part, de rechercher la responsabilité de l'hébergeur[355]. Toutefois, l'hébergeur ne sera tenu responsable que seulement si l'information ou l'activité présente un caractère

---

[350] En vertu de l'article 6-I-5 de la *LCEN* qui énonce ce qui suit : « 5. La connaissance des faits litigieux est présumée acquise par les personnes désignées au 2 lorsqu'il leur est notifié les éléments suivants :

- la date de la notification ;
- si le notifiant est une personne physique : ses nom, prénoms, profession, domicile, nationalité, date et lieu de naissance ;
- si le requérant est une personne morale : sa forme, sa dénomination, son siège social et l'organe qui la représente légalement ;
- les noms et domicile du destinataire ou, s'il s'agit d'une personne morale, sa dénomination et son siège social ;
- la description des faits litigieux et leur localisation précise ;
- les motifs pour lesquels le contenu doit être retiré, comprenant la mention des dispositions légales et des justifications de faits ;
- la copie de la correspondance adressée à l'auteur ou à l'éditeur des informations ou activités litigieuses demandant leur interruption, leur retrait ou leur modification, ou la justification, de ce que l'auteur ou l'éditeur n'a pu être contacté ».

[351] *Mme M. B., M. P.T., M. F .D. c/ Wikimedia Foundation Inc., précitée*, note 182 ; Lionel THOUMYRE, « L'art et la manière de notifier l'hébergeur 2.0 », Études n° 5, Communication Commerce Électronique, février 2008, p. 18 s.; *Les Arnaques.com* c / *Ed. régionales de France*, CA de Versailles, 12 décembre 2007.

[352] Lionel THOUMYRE, « La responsabilité pénale et extracontractuelle des acteurs de l'Internet », *loc. cit.*, note 169 ; Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit..*, note 47, p. 24 ; Julien TAÏEB, « Prestataires techniques de l'Internet : le sens des responsabilités », *loc. cit*, note 105, p. 7.

[353] En vertu de l'article 6-I-4 de la *LCEN* qui dispose que « [l]e fait, pour toute personne, de présenter aux personnes mentionnées au 2 un contenu ou une activité comme étant illicite dans le but d'en obtenir le retrait ou d'en faire cesser la diffusion, alors qu'elle sait cette information inexacte, est puni d'une peine d'un an d'emprisonnement et de 15 000 EUR d'amende. »

[354] En vertu de l'article 6-I-4 de la *LCEN* : voir *supra*, note, 353 ;

[355] *ibid* ; Julien TAÏEB, « Prestataires techniques de l'Internet : le sens des responsabilités », *loc. cit*, note 105, p. 7.

« *manifestement illicite* »[356]. Dans une décision du 10 juin 2004[357], le Conseil constitutionnel a estimé dans la réserve d'interprétation visant à restreindre les cas de mise en œuvre de la responsabilité des intermédiaires techniques que les articles 6-1-2 et 6-1-3 de la *LCEN* « *ne sauraient avoir pour effet d'engager la responsabilité d'un hébergeur qui n'a pas retiré une information dénoncée comme illicite par un tiers si celle-ci ne présente pas manifestement un tel caractère ou si son retrait n'a pas été ordonné par un juge* ». Selon l'interprétation donnée par le Conseil Constitutionnel, l'expression « *manifestement illicite* » ne doit viser que les contenus d'une gravité manifeste, tels que les propos racistes ou des images pédopornographiques[358] et qu'« *en aucun cas les atteintes au code de la propriété intellectuelle ne pourraient être considérées comme un cas manifeste* »[359]. Pourtant, la jurisprudence a ouvert la porte du « *manifestement illicite* » et semble à même d'accueillir les contenus portant atteinte au droit d'auteur ou à l'intimité de la vie privée[360]. Ainsi, à plusieurs reprises[361], *Google* a été condamné pour avoir refusé de retirer de l'information dont le contenu

---

[356] Pierre TRUDEL, « La responsabilité sur Internet en droit civil québécois », *loc. cit.*., note 47, p. 24 ; Julien TAÏEB, « Prestataires techniques de l'Internet : le sens des responsabilités », *loc. cit*, note 105, p. 5.

[357] *Décision du Conseil Constitutionnel* du 10 juin 2004, n°2004-496, en ligne sur le site du Conseil Constitutionnel: < http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/depuis-1958/decisions-par-date/2004/2004-496-dc/decision-n-2004-496-dc-du-10-juin-2004.901.html > (visité le 19 février 2009) ; Voir Ophélie FONDEVILLE et Anne-Sophie JOUANNON, « Le 'manifestement illicite', mystérieux point de rencontre entre la victime et l'hébergeur » Juriscom.net, 7-04-2008, en ligne sur : < http://www.juriscom.net/pro/visu.php?ID=1051 > (visité le 19 février 2009).

[358] *Décision du Conseil Constitutionnel* du 10 juin 2004, n°2004-496, en ligne sur le site du Conseil Constitutionnel: < http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/depuis-1958/decisions-par-date/2004/2004-496-dc/decision-n-2004-496-dc-du-10-juin-2004.901.html > (visité le 19 février 2009) ; Forum des droits sur l'Internet, Recommandation du Forum des droits sur l'internet « Les Enfants du Net (2) – Pédopornographie et pédophilie sur l'internet », 25 janvier 2005, en ligne sur : < http://www.foruminternet.org/specialistes/concertation/recommandations/recommandation-du-forum-des-droits-sur-l-internet-les-enfants-du-net-2-pedo-pornographie-et-pedophilie-sur-l-internet.html > (visité le 19 février 2009) ; Alain Afflelou c/ Google, Free, Tribunal de grande instance de Paris, Ordonnance de référé du 27 février 2006, en ligne sur Legalis.net : < http://www.legalis.net/jurisprudence-decision.php3?id_article=1648> (visité le 19 février 2009). À ce sujet, voir Etienne WÉRY, « La notion de contenu manifestement illicite soumise au juge des référés », 15/02/2007, en ligne sur : < http://www.droit-technologie.org/actuality-1008/la-notion-de-contenu-manifestement-illicite-soumise-au-juge-des-refere.html > (visité le 19 février 2009).

[359] Il s'agit de l'avis émis par le Secrétaire Général du Conseil constitutionnel lors d'une explication du texte pour la presse, le 15 juin 2004 : Jérôme THOREL, « *LCEN* : le SNEP désapprouve en partie l'avis du Conseil Constitutionnel », Zdnet.fr, 22/06/2004, en ligne sur : < http://www.zdnet.fr/actualites/telecoms/0,39040748,39157926,00.htm > (visité le 19 février 2009).

[360] *Google* c/ *Zadig productions*, *précitée*, note 142; décision *Google* c/ *Flach Films*, Tribunal de commerce de Paris, 8ème chambre, Jugement du 20 février 2008, en ligne sur : < http://www.legalis.net/jurisprudence-decision.php3?id_article=2223 > (visité le 19 février 2009) ; *Google Inc / Benetton*, Bencom, *précitée*, note 172 ; *SARL Lycos France* c. *Abdelhadi S. et SA Dounia et SAS iEurope* CA Paris, 6 juin 2007, en ligne sur : < http://www.lasic.fr/public/cspla/36.pdf > (visité le 19 février 2009) ; Julien TAÏEB, « Prestataires techniques de l'Internet : le sens des responsabilités », *loc. cit*, note 105, p. 6.

[361] *Google* c/ *Zadig productions*, *précitée*, note 142; décision *Google* c/ *Flach Films*, Tribunal de commerce de Paris, 8ème chambre, Jugement du 20 février 2008, en ligne sur : < http://www.legalis.net/jurisprudence-decision.php3?id_article=2223 > (visité le 19 février 2009) ; *Google Inc / Benetton*, Bencom, *précitée*, note 172.

portait atteinte à des droits de propriété intellectuelle. Dans la décision *SARL Lycos France* c. *Abdelhadi S. et SA Dounia et SAS iEurope* [362]., la Cour d'appel de Paris a estimé que « *des propos portant de façon évidente atteinte à l'intimité de la vie privée, en ce qu'ils ne nécessitent pas d'enquête ou de vérification préalable pour que soit constatée leur illicéité, constituent un contenu manifestement illicite* ». Par conséquent, ces décisions témoignent de la volonté des tribunaux de faire de l'hébergeur un « *juge à la place du juge* »[363] en le contraignant à toujours s'assurer du caractère licite des contenus qu'il diffuse[364].

Deuxièmement, la connaissance peut résulter d'un *ensemble de faits ou de circonstances rendant apparent le caractère d'illicéité*. À cet égard, l'hébergeur sera bien malaisé de procéder à la suppression de contenus qui ne présentent pas un cas absolument clair d'illicéité. En effet, sur la base de quelle autorité cet intermédiaire doit-il se baser pour décider qu'une telle information ou activité possède ou non un caractère illicite ? Par ailleurs, dans des situations qui prennent une dimension politique, peut-on s'attendre d'un hébergeur à ce qu'il juge du caractère illicite d'une information ou activité ? À titre d'exemple, dans l'affaire du génocide arménien[365], le TGI et la Cour d'appel de Paris avaient jugé que les contenus niant un génocide n'étaient pas « *manifestement illicites* ». Il n'appartient pas à l'hébergeur de répondre à des questions aussi difficiles et lourdes de conséquences que celle-ci[366]. Par conséquent, il est évident que l'hébergeur peut se retrouver en difficulté face à des contenus pour lesquels il s'avère difficile de déterminer son caractère illicite[367]. Dans les situations qui ne permettent pas à l'hébergeur de trancher, cet intermédiaire ne doit pas hésiter à solliciter l'aide d'un juge afin d'éviter d'éventuelles erreurs ou tout simplement, pour confirmer le caractère litigieux d'une information ou activité[368].

---

[362] CA Paris, 6 juin 2007, en ligne sur : < http://www.lasic.fr/public/cspla/36.pdf > (visité le 19 février 2009).
[363] Lionel THOUMYRE, « Précisions contrastées sur trois notions clés relatives à la responsabilité des hébergeurs », *loc. cit.*, note 271, p. 17-20.
[364] Julien TAÏEB, « Prestataires techniques de l'Internet : le sens des responsabilités », *loc. cit*, note 105, p. 6.
[365] *Comité de défense de la cause arménienne* c/ *M. Aydin S.*, TGI de Paris, 15 novembre 2004, et Cour d'Appel de Paris, 8 novembre 2006, France Télécom services de communication résidentiels. Dans cette affaire, le Consulat Général de Turquie avait publié sur son site Web des documents concernant le génocide arménien. Le Comité de Défense de la Cause Arménienne avait assigné en justice le Consulat et son hébergeur.
[366] *Comité de défense de la cause arménienne* c/ *M. Aydin S*, précitée, note, 365 ; Julien TAÏEB, « Prestataires techniques de l'Internet : le sens des responsabilités », *loc. cit*, note 105, p. 7.
[367] Julien TAÏEB, « Prestataires techniques de l'Internet : le sens des responsabilités », *loc. cit*, note 105, p. 7.
[368] *ibid*, p. 7-8.

La *LCEN* met à la charge de l'hébergeur une obligation *a posteriori*, celle d'agir une fois cette connaissance acquise. La même disposition[369] contraint ce dernier à *agir promptement pour retirer les informations présentant un caractère illicite ou en rendre l'accès impossible*, à partir du moment *où il en a une connaissance effective* ou présumée. La *LCEN* détermine dans cette disposition le point de départ de l'obligation d'agir de l'hébergeur. Ainsi, dans l'affaire *Lacoste*[370], le TGI de Nanterre a soulevé que l'hébergeur devait mettre en place une procédure permettant de retracer l'auteur du site litigieux afin de le mettre en demeure de se conformer à ses obligations ou lui donner l'occasion de justifier ses prétentions sur la licéité de l'information avant de procéder au retrait en tant que tel. Cette obligation d'agir se dégageait également de la *Directive sur le commerce électronique*.

En deuxième lieu, il y a lieu d'analyser la disposition qui prévoit le principe de connaissance à l'égard du transmetteur[371]. Contrairement à la disposition qui traite de l'hébergeur, celle qui vise le transmetteur n'énonce pas explicitement le principe de connaissance. Toutefois, il faut avoir recours à un effort d'interprétation afin d'arriver à soulever le principe de connaissance qui se présente de manière implicite dans la disposition. Celle-ci comporte des cas de figure se rattachant à l'idée de contrôle exercée par l'intermédiaire sur l'activité ou information litigieuse. Ainsi, la responsabilité du transmetteur peut être engagée *dans les cas où soit [il] est à l'origine de la demande de transmission litigieuse, soit [il] sélectionne le destinataire de la transmission, soit [il] sélectionne ou modifie les contenus faisant l'objet de la transmission*. Puisque être à l'origine de la transmission ou modifier les contenus s'y reliant impliquent pour le transmetteur de connaître le contenu de l'information qu'il transmet. Sélectionner le destinataire de la transmission suppose une connaissance du nom de la personne à qui sera envoyé le contenu illicite. Tout comme c'était le cas pour la *Directive sur le commerce électronique* et contrairement à la *Convention sur la cybercriminalité*, le principe de connaissance se dégage de manière implicite dans la *LCEN*.

---

[369] En vertu des articles 6-I-2 et 6-I-3 de la *LCEN*.

370 *Lacoste* c. *SA Multimania Production et a.*, TGI Nanterre, 1er ch. A., 8 décembre 1999, J.C.P. 2000.II.102. Au titre de cette obligation et afin de prévenir toute récidive, le Tribunal condamne ce dernier à mettre en place un système permettant de retracer les sites litigieux et de les supprimer.

[371] En vertu de l'article 9 de la *LCEN*. (Article L. 32-3-3° du *Code des postes et des communications électroniques*). Il y a également l'article 6-I-1° de la *LCEN* qui prévoit la nécessité pour ce dernier d'informer ses abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens..

En troisième lieu, il y a lieu d'analyser la disposition qui traite du principe de connaissance à l'égard de l'intermédiaire assurant une activité de stockage dans le seul but de rendre plus efficace la transmission ultérieure de l'information[372]. Parallèlement à la disposition visant l'hébergeur et contrairement à la disposition qui concerne le transmetteur, celle-ci traite expressément du principe de connaissance. Aux termes de cette disposition[373], cet intermédiaire peut engager sa responsabilité civile s'il n'a pas agit *avec promptitude pour retirer les contenus [qu'il a] stockés ou pour en rendre l'accès impossible, dès qu'[il] a effectivement eu connaissance,* a) *soit du fait que les contenus transmis initialement ont été retirés du réseau*, b) *soit du fait que l'accès aux contenus transmis initialement a été rendu impossible*, c) *soit du fait que les autorités judiciaires ont ordonné de retirer du réseau les contenus transmis initialement ou d'en rendre l'accès impossible.* À la différence de la disposition traitant de l'hébergeur, celle-ci n'érige de responsabilité que sur le plan civil. La disposition se rapporte uniquement à la *connaissance effective* alors que celle qui dispose de l'hébergeur se rattache également à la connaissance découlant des faits ou circonstances rendant apparente le caractère illicite de l'information ou activité. À cet égard, les commentaires formulés précédemment à l'égard de l'hébergeur au sujet de la *connaissance effective* s'appliquent également pour cet intermédiaire. Au titre de cette disposition[374], son obligation d'agir commence dès qu'il est mis au courant de la survenance de l'un des événements édictés dans celle-ci. Cette obligation *a posteriori* mise à la charge de cet intermédiaire est similaire à celle qui ressortait de la disposition visant l'hébergeur.

En résumé, l'on a vu que la loi française édicte expressément le principe de connaissance dans les dispositions qui traitent de l'hébergeur et de l'intermédiaire assurant une activité de stockage automatique dans le seul but de rendre plus efficace la transmission ultérieure de l'information[375] et ce, parallèlement à la *Directive sur le commerce électronique* et contrairement à la *Convention sur la cybercriminalité*. La disposition visant le transmetteur n'inclut ce principe que de manière implicite. L'on a

---

[372] En vertu de l'article 9 de la *LCEN*. (Article L. 32-3-4° du *Code des postes et des communications électroniques*).
[373] *ibid.*
[374] En vertu de l'article 9 de la *LCEN*. (Article L. 32-3-4° du *Code des postes et des communications électroniques*).
[375] En vertu de l'article 6-I-2° de la *LCEN* et en vertu de l'article 9-I de la *LCEN*. (Article L. 32-3-4-2° du *Code des postes et des communications électroniques*).

dégagé deux formes de connaissance : la *connaissance réelle* et la *connaissance présumée*. Dans le premier cas, elle émane de l'intermédiaire ou d'une tierce partie alors que dans le deuxième cas, elle provient d'une série d'éléments rendant apparente la présence d'une activité ou information illicite. L'on a constaté que l'interprétation fournie par les autorités sur le caractère « *manifestement illicite* » de l'information n'était pas suivie dans la jurisprudence qui est d'ailleurs enclin à contraindre l'hébergeur à juger du caractère illicite du contenu. L'on a alors vu que cette situation a amené cet intermédiaire à s'interroger sur les véritables obligations qui sont mises à son encontre en matière de retrait du contenu litigieux. L'on a observé qu'à la différence de la *Directive sur le commerce électronique*, la *LCEN* mettait en place une procédure rigoureuse de notification. L'on a remarqué que la connaissance constituait le point de départ de la responsabilité des intermédiaires techniques en ce qu'elle annonce le moment à partir duquel ils doivent agir. Cette obligation d'agir avec promptitude se matérialise par le retrait immédiat du contenu illicite ou par la cessation de l'activité en question.

En conclusion, la loi française prête à une rédaction plus précise et plus rigoureuse du principe de connaissance que la *Directive sur le commerce électronique*. En outre, elle est plus pragmatique puisqu'elle comporte des modalités de sanctions pénales et ce, contrairement aux autres instruments juridiques nationaux et internationaux. Par conséquent, le principe de connaissance s'imprègne de la loi française comme un critère d'imputabilité applicable aux seuls intermédiaires suivants : l'hébergeur, l'intermédiaire assurant une activité de stockage automatique dans le seul but de rendre plus efficace la transmission ultérieure de l'information et le transmetteur.

Après avoir analysé la loi française, il convient maintenant de faire le même exercice pour la législation américaine.

D) Le *Communications Decency Act* américain

Dans cette section, il convient d'examiner la notion de connaissance qui se dégage de la l'article 230(c)(1) de *Communications Decency Act*[376]. La notion de

[376] Voir, *supra,* note 18. Cette disposition écarte la responsabilité des utilisateurs d'un service informatique interactif et des fournisseurs d'accès Internet pour la tenue et la transmission de propos illicites par le biais de

connaissance ne s'applique pas aux fournisseurs d'accès Internet alors qu'il n'en est pas ainsi dans les autres instruments juridiques. À titre d'exemple, dans une décision opposant Kenneth Zeran à *America Online*[377], la Cour a conclu, sur le fondement du *Communications Decency Act*, que *AOL* ne pouvait être tenu responsable des dommages causés en raison des informations publiées sur son serveur commercial et émanant d'un tiers, malgré qu'il soit mis au courant de la teneur de ces informations. La Cour a considéré qu'une personne qui offre un service de connexion à un ou plusieurs services de communication ne peut être assimilée aux autres diffuseurs d'informations, comme par exemple, les éditeurs de journaux, magazines, la télévision car ces derniers exercent un contrôle effectif sur l'information véhiculée alors que le fournisseur de services Internet ne peut contrôler efficacement et rapidement le contenu de l'information. Et dans l'hypothèse où ce fournisseur aurait tout simplement retiré volontairement les messages illégaux, la Cour estime que ce dernier ayant agit en « *bon samaritain* » demeurerait non-responsable. Cette conception du législateur américain se concilie difficilement avec l'approche française et québécoise qui privilégie une protection accrue à l'endroit des tiers. Ainsi, selon la logique de ces deux lois, à partir du moment où l'intermédiaire obtient la confirmation indépendante du fait de la présence d'activités illicites par le biais de ses services, il doit agir afin de faire cesser la poursuite de l'activité illicite, à défaut de quoi il sera considéré comme étant un agent actif et devra alors supporter la responsabilité qui en découle, étant donné que son rôle de simple transmetteur se transforme ainsi en un véritable éditeur de l'information. Cette approche trop libérale de la loi américaine peut mener à des conséquences désastreuses, notamment la multiplication des activités illicites

---

l'Internet : « *No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.* ». En vertu de cette disposition, ces intermédiaires peuvent, de leur propre initiative, prendre des moyens en vue de supprimer le contenu litigieux ou de restreindre l'accès ou la disponibilité de matériel qu'ils considèrent obscène. Au titre de cette immunité, ils n'ont aucune obligation de supprimer les contenus illicites circulant par le biais de leurs réseaux, ils peuvent toutefois décider de le faire volontairement et à partir de ce moment, ils seront tout simplement considérés comme agissant en bon samaritain : *Communication Decency Act*, 47 U.S.C s. 230(c)(1) énonce ce qui suit : « TREATMENT OF PUBLISHER OR SPEAKER- No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider. ». La Loi oblige également les manufacturiers de télévision à installer des équipements qui permettront aux téléspectateurs de bloquer certaines émissions, en raison de leur qualification : Pierre Trudel et Karim Benyekhlef, « Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes », *loc. cit.*, note 283, p. 24. Contrairement à la *Convention sur la cybercriminalité* et parallèlement à la loi québécoise, la loi américaine aménage un régime de responsabilité qui ne s'applique pas sur le plan criminel.

[377] *Kenneth M. Zeran* c. *America Online, Inc.*, *précitée*, note 290.

commises sur le réseau Internet, notamment par la prolifération de messages à contenus illicites sur Internet, sans que l'on puisse faire cesser la poursuite de ces activités[378].

La notion de connaissance ne s'applique généralement[379] pas à l'égard du fournisseur d'hébergement. Les décisions américaines enseignent que l'immunité édictée par la loi ne joue que lorsque l'utilisateur d'un service informatique interactif se qualifie de fournisseur d'hébergement –ou de fournisseur d'accès Internet, comme vu plus haut. À titre d'exemple, dans l'affaire *Carafano*[380], la Cour a qualifié *Matchmaker* de fournisseur d'hébergement en estimant que l'utilisateur était le seul à compléter le contenu du profil à l'aide du questionnaire à choix multiples. Par conséquent, la Cour a conclu que « *Matchmaker ne pouvait être tenu responsable, de l'association de certaines réponses à choix multiples avec un ensemble de caractéristiques physiques et une photographie* ».

Par contre, il existe une certaine tendance dans la jurisprudence américaine à faire appliquer la notion de connaissance à l'égard du fournisseur d'hébergement. Cette notion ressort de l'interprétation de cette disposition qui prévoit que l'immunité est inopérante à l'égard de tout utilisateur d'un service informatique interactif jouant le rôle de l'éditeur[381]. Et l'alinéa f) de cette disposition édicte que l'expression « *information content provider* » constitue « *any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service* ». Toute personne qui contribuerait en partie ou en totalité en la création et le développement de l'information fournie par le biais de services Internet se retrouverait ainsi à exercer un certain contrôle sur l'information ou activité en question, d'où la fonction de l'éditeur. Ce qui impliquerait alors une connaissance de la nature illicite de l'information ou activité. À titre d'exemple, dans

---

[378] Comme l'indique l'auteur Nathalie Boulvard qui critique cette disposition : « Les victimes sont seules face à des délinquants inconnus et des fournisseurs d'accès drapés dans leur immunité ! Les juges américains, pourront-ils soutenir, encore longtemps, l'irresponsabilité des fournisseurs d'accès en qualifiant d'actes de "bon samaritain" leurs ponctue-les et discrétionnaires coopérations? »: Nathalie BOULVARD, « *États-Unis* -Dérives sur Internet : immunité des fournisseurs d'accès », Expertises des systèmes d'information, n°218, Septembre 1998, en ligne sur : < http://www.celog.fr/expertises/1998/som0898/immunite0898.htm > (visité le 28 juin 2008).

[379] Le courant majoritaire applique l'immunité prévue par la loi au fournisseur d'hébergement et ce, même si ce dernier a un rôle structurant dans la présentation de son site Web.

[380] *Carafano* c. *Metrosplash.com Inc.*, *préciée*, note 129. L'opérateur du site *Matchmaker.com* qui offre un service de rencontre matrimonial à ses membres est poursuivi sur la base d'atteinte à la vie privée. Les membres peuvent y créer leur propre profil à l'aide d'un questionnaire. Forum des droits sur l'Internet, « États-Unis: extension du régime de responsabilité allégée aux agences matrimoniales virtuelles », *loc. cit*, note 148.

[381] En vertu de l'article 230(c)(1) de *Communications Decency Act*.

l'affaire *Fair Housing Council of San Fernando Valley*[382], la Cour devait se prononcer sur la qualification de *Rommate*, un site qui propose d'offrir à ses membres des services de colocation à l'aide d'outils techniques permettant la création de profils personnels. Dans cette décision, l'hébergeur a été poursuivi par avoir contrevenu aux lois relatives à la discrimination en matière de logement. À cet égard, la Cour a établi que *Rommate* se qualifiait de fournisseur de contenus[383], en estimant qu'il pose des actes qui sont de nature à structurer, en partie ou en totalité, le contenu de l'information provenant de ses membres[384]. Elle a soutenu que pour se qualifier à ce titre, il ne devait jouer de rôle actif quant au contenu de l'information à être publiée par le biais de son serveur. Elle a ensuite conclu qu'il ne pouvait par conséquent se prévaloir de l'immunité prévue par la loi.

En résumé, le législateur américain adopte donc une position marginale au sujet de la responsabilité des intermédiaires techniques en instaurant un régime d'immunité très large. À ce sujet, il se distingue nettement des législateurs français, québécois et européen qui, quant à eux, consacrent un régime d'exonération de responsabilité conditionnelle. Contrairement aux lois française et québécoise, cette loi américaine ne prévoit pas de mécanismes de notification. Par contre, tout comme ces deux législations, il ne couvre pas le domaine de la responsabilité criminelle.

En conclusion, le droit américain se montre alors incomplet par rapport aux autres instruments juridiques en ce qui concerne l'interprétation du principe de connaissance comme critère d'imputabilité applicable aux intermédiaires techniques. Il s'annonce comme celui manquant le plus de rigueur puisqu'il ne tient toujours pas compte de cette notion pour évaluer l'imputation de responsabilité des utilisateurs d'un service informatique interactif, notamment le fournisseur d'hébergement. Toutefois, il applique ce principe à l'égard du fournisseur de contenus.

---

[382] *Fair Housing Council of San Fernando Valley* c. *Roommate.com*, LLC, *précitée*, note 145. Il faut préciser que cette décision ne représente pas le courant majoritaire qui ne considère généralement pas le rôle structurant que joue l'hébergeur sur l'information ou activité en question.

[383] La Cour s'exprime comme suit: « A content provider is « any person or entity that is responsible, *in whole or in part*, for the creation or development of information provided through the Internet." 47 U.S.C. § 230(f)(3).

[384] Si à l'inverse, l'opérateur du site Roommate.com, ne faisait que publier passivement l'information qu'il reçoit de ses membres, il serait alors considéré comme un simple fournisseur d'hébergement et serait visé par cette immunité : *Fair Housing Council of San Fernando Valley* c. *Roommate.com*, LLC, *précitée*, note 145. Voir également *Batzel* c. *Smith*, *précitée*, note 147.

Il y a lieu de généraliser les principaux points qui ressortent de l'étude du principe de connaissance à travers ces différents textes nationaux et internationaux. Qu'il soit ou non prévu comme étant spécifiquement applicable à chacun d'eux, ce principe s'articule comme un critère permettant d'évaluer globalement l'imputation de responsabilité des intermédiaires techniques.

Après avoir analysé le principe de connaissance à l'intérieur de plusieurs législations, l'on examinera dans la prochaine section la notion de l'absence d'obligation légale de surveillance.

Section III- L'absence d'obligation légale de surveillance

Dans cette section, il convient d'examiner la notion de l'absence d'obligation légale de surveillance. Cette notion se rattache au fait pour les intermédiaires techniques de ne pas être soumis à une obligation de surveillance active sur l'information, ni de rechercher des circonstances indiquant que les documents permettent la réalisation d'activités illicites[385]. Elle a pour corollaire que ces derniers ne doivent prendre aucun moyen pour empêcher la personne responsable de l'accès aux documents d'exercer ses fonctions, notamment en ce qui a trait à la confidentialité et ils ne doivent non plus prendre aucun moyen pour empêcher les autorités responsables d'exercer leurs fonctions, en vertu des pouvoirs que leur confère la loi, relativement à la sécurité publique ou à la prévention, à la détection, à la preuve ou à la poursuite d'infractions. Ainsi, l'exclusion de l'obligation légale de surveillance applicable aux intermédiaires comporte une condition, celle de ne pas s'interférer dans les fonctions des personnes responsables de l'accès aux documents, plus précisément de la confidentialité des informations. Ils ne doivent également pas s'ingérer dans les fonctions des forces de l'ordre relativement à la sécurité publique, à la prévention et à la détection et à la poursuite d'infractions. En cas du non-respect de ces conditions, les intermédiaires ne pourraient plus bénéficier de l'exemption d'obligation légale de surveillance, se trouvant ainsi à jouer un rôle actif dans la transmission de l'information.

---

[385] Pierre TRUDEL, « La responsabilité des acteurs du commerce électronique », *loc. cit.*, note 8, p. 623.

Dans cette perspective, plusieurs textes législatifs, que ce soit au niveau national ou international, prévoient l'exclusion de l'obligation légale de surveillance. Dans cette section, il faut analyser les différents textes législatifs qui consacrent ce principe, à savoir la *Convention sur la cybercriminalité* ainsi que le Protocole additionnel, la *Directive sur le commerce électronique*, les lois française et américaine.

A) La *Convention sur la cybercriminalité*

Tout d'abord, il faut amorcer l'étude de ce principe avec la *Convention sur la cybercriminalité* ainsi que le Protocole additionnel.

Tout d'abord, commençons avec la Convention. Cet instrument juridique prévoit des dispositions qui ne s'appliquent qu'à l'auteur du crime. Seule la disposition visant la complicité se trouve directement applicable aux intermédiaires techniques[386]. Contrairement aux autres instruments juridiques nationaux et internationaux, sauf la loi américaine, la Convention n'énonce pas expressément le principe de l'absence de l'obligation légale de surveillance. Toutefois, la lecture du rapport explicatif de la Convention nous enseigne que ce principe est tout de même visé par la disposition traitant de la complicité. À cet égard, le rapport explicatif énonce ce qui suit : « *Les fournisseurs de services ne sont donc pas tenus de surveiller activement le contenu pour éviter la responsabilité pénale en vertu de cette disposition* »[387]. Ainsi, en vertu de cette disposition, le prestataire agissant à titre de fournisseur de services sur un réseau de communication n'est pas tenu de surveiller l'information, ni de rechercher les circonstances indiquant que les données informatiques servant à la réalisation d'activités illicites. Même si le texte interprétatif fournit un exemple qui ne vise que le fournisseur de services, il est loisible d'appliquer ce principe, sur la base du même raisonnement, à l'égard des autres intermédiaires, à savoir celui agissant comme un intermédiaire offrant des services de référence à des documents technologiques ou comme un intermédiaire conservant les documents à la seule fin d'assurer l'efficacité de leur transmission ultérieure. Puisqu'ils sont tous des acteurs qui ne contrôlent *a*

---

[386] En vertu de l'article 11 de la Convention.

[387] *Convention sur la cybercriminalité*, Rapport explicatif, *loc. cit.*, note 24, par. 119. Voir également le paragraphe 105 du rapport explicatif qui mentionne ce qui suit : « De plus, un fournisseur de services n'est pas tenu de surveiller le contenu pour éviter la responsabilité pénale » : *Convention sur la cybercriminalité*, Rapport explicatif, *loc. cit.*, note 24, par. 105.

priori pas les activités se déroulant sur Internet[388]. Ainsi, ces deux intermédiaires, tout comme le fournisseur de services, ne sont pas tenus de vérifier le contenu de l'information qui est échangé sur le réseau Internet.

Le principe de l'absence d'obligations légale de surveillance comporte deux volets. Tout d'abord, il implique le droit pour les intermédiaires de ne pas surveiller activement le contenu des communications. Ensuite, il suppose l'obligation pour ces derniers de ne pas faire de surveillance active sur les communications électroniques, de façon à ne pas perturber le cours normal de la circulation de l'information sur Internet. Cette compréhension du principe de l'absence d'obligation légale de surveillance se veut compatible avec les autres instruments juridiques qui lui donnent une interprétation faisant ressortir les deux composantes de ce principe, à savoir le droit de ne pas surveiller mais aussi l'obligation de ne pas surveiller les informations ou activités illicites se déroulant sur Internet.

Deuxièmement, examinons le Protocole. Ce texte international, tout comme la Convention comporte des dispositions qui ne visent que l'auteur du crime, à l'exception d'une seule qui s'applique directement aux intermédiaires techniques, à savoir celle liée à la complicité[389]. Cette disposition ne traite pas expressément du principe d'absence d'obligation légale de surveillance. Toutefois, il se dégage de son texte interprétatif qui reprend essentiellement les termes employés dans la Convention au sujet de ce principe[390]. À cet égard, le rapport formule ce qui suit : « *Les fournisseurs de services ne sont donc pas tenus de surveiller activement le contenu pour éviter la responsabilité pénale en application de cette disposition* »[391]. Ainsi, en vertu de la disposition concernant la complicité, les intermédiaires ne sont pas tenus de procéder à

---

[388] Si ces intermédiaires ne contrôlent pas les activités se déroulant sur Internet, ils ne peuvent alors pas surveiller le déroulement de celle-ci. De plus, la responsabilité des intermédiaires ne commence qu'à partir du moment où ils ont connaissance du contenu litigieux de l'information ou des circonstances donnant lieu à croire que les documents permettent la réalisation d'activités illicites. Ce qui suppose que l'intermédiaire doit agir de façon neutre avant l'envoi de toute notification indiquant la présence d'activités illicites, de sorte que ses agissements ne doivent relever d'aucune ingérence dans les communications électroniques. Ainsi, tant qu'il n'a pas effectivement connaissance d'activités illégitimes, il ne doit prendre aucun moyen pour empêcher les usagers d'accéder à des documents sur Internet ou pour empêcher les autorités nationales d'exécuter leurs fonctions conformément à la loi.

[389] En vertu de l'article 7 du Protocole.

[390] *Convention sur la cybercriminalité*, Rapport explicatif, *loc. cit.*, note 24, par. 105, 119.

[391] *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, Rapport explicatif, *loc. cit.*, note 28, par. 45. Voir également le paragraphe 25 qui énonce ce qui suit : « *De plus, un fournisseur de service n'est pas tenu de surveiller le contenu pour éviter la responsabilité pénale* » : *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, Rapport explicatif, *loc. cit.*, note 28, par. 25.

une surveillance active des activités se déroulant par le biais de leurs installations. Parallèlement au rapport interprétatif de la Convention, celui du Protocole n'applique ce principe qu'à l'égard du fournisseur de services. Toutefois, il est possible d'affirmer que ce principe s'applique également aux autres intermédiaires techniques[392].

Tout comme la Convention, le Protocole considère que ce principe comporte deux acceptions. La première se rapporte au droit de ne pas surveiller les communications, et la deuxième à l'obligation de ne pas s'ingérer dans le cycle de l'information, à partir du point de départ de l'information jusqu'à son point de l'expédition.

Après l'analyse des deux instruments juridiques, il y a lieu de faire les constatations suivantes. Le principe de l'absence de l'obligation légale de surveillance se dégage implicitement des dispositions visant la complicité[393]. Au titre de cette disposition, les intermédiaires techniques n'ont *a priori* pas l'obligation de surveiller le contenu des communications qui transigent par le biais de ses services. Ce principe est compris dans ces deux textes en tant que concept comportant double sens. D'un côté, il est perçu comme le « *droit* » de ne pas procéder à de la surveillance active, et, d'un autre côté, comme l'« *obligation* » de ne pas s'interférer dans les communications électroniques. La compréhension par ces instruments juridiques de ce principe s'apparente aux autres instruments juridiques qui l'interprètent comme renfermant ce double sens.

En conclusion, la Convention et le Protocole comprennent le principe de l'absence d'obligation légale de surveillance comme un critère d'imputabilité applicable aux intermédiaires techniques.

Après avoir examiné la Convention et le Protocole, faisons maintenant le même exercice pour la loi française.

---

[392] À cet égard, il y a lieu de se référer au raisonnement invoqué ci-haut dans le paragraphe qui porte sur l'analyse du principe de l'absence d'obligation légale de surveillance dans la Convention.
[393] En vertu de l'article 11 de la Convention et de l'article 7 du Protocole.

B) La *Directive sur le commerce électronique*

Dans cette section, il faut analyser les dispositions de la *Directive sur le commerce électronique*[394] qui énoncent expressément[395] le principe de l'absence d'obligation légale de surveillance afin de savoir comment il s'articule dans le texte par rapport aux autres instruments juridiques. Aux termes de ce principe, les intermédiaires techniques sont tenus, pour la fourniture des services visant le simple transport, le stockage et l'hébergement de l'information, de ne pas surveiller activement les informations qu'ils transmettent ou stockent ou de ne pas rechercher activement des faits ou des circonstances révélant des activités illicites[396]. L'on remarque une rédaction qui privilégie une approche mettant sur le même pied d'égalité ce principe à l'égard de ces trois intermédiaires, à savoir le transmetteur, l'archiveur et l'hébergeur. À cet égard, le législateur québécois[397] se rallie au législateur européen en prévoyant dans le même libellé la responsabilité de ces trois intermédiaires techniques. De ce constat, il est possible de déduire que la *Directive sur le commerce électronique* organise le régime de responsabilité de chacun des intermédiaires techniques de façon différente pour les trois principes puisqu'elle traite le principe de l'absence d'obligation légale de surveillance de manière homogène pour chacun des trois intermédiaires alors qu'elle fait des nuances entre chacun des intermédiaires techniques pour ce qui est du principe de contrôle et de connaissance. En outre, la *Convention sur la cybercriminalité* renferme également ce principe par le biais de son texte interprétatif.

---

[394] Voir, *supra*, note 15. Rappelons que le texte européen instaure au sein du « *Marché intérieur* » un cadre juridique européen qui, d'une part, garantit la sécurité juridique entre les entreprises et les consommateurs et, d'autre part, assure des règles harmonisées qui portent sur la transparence des communications commerciales en ligne, la conclusion de contrats électroniques et le régime de responsabilité devant s'appliquer aux prestataires de services. Par ailleurs, la *Directive sur le commerce électronique* consacre un régime de responsabilité réduite qui rend *a priori* non-responsable les intermédiaires techniques tout en énumérant les cas dans lesquels la responsabilité de l'intermédiaire peut être engagée : voir les articles 12, 13 et 14 de la *Directive sur le commerce électronique*. De plus, tout comme les lois française et québécoise, la *Directive sur le commerce électronique* module le régime de responsabilité en fonction du rôle joué par chacun des intermédiaires, à l'exception de la responsabilité qui incombe à l'intermédiaire fournissant des services de référence à des documents technologiques. En outre, elle dispense les prestataires de services de procéder *a priori* à des contrôles systématiques, ce que l'on appelle l'absence d'obligation légale de surveillance : voir l'article 15 et Considérant 47.

[395] Le premier paragraphe de l'article 15 de la *Directive sur le commerce électronique* énonce ce qui suit : « Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites ». Rappelons que ce principe se dégage également expressément des lois française et québécoise et ce, à la différence de la *Convention sur la cybercriminalité* qui ne le consacre qu'implicitement.

[396] En vertu de l'article 15 de la *Directive sur le commerce électronique*.

[397] En vertu de l'article 27(1) de la *LCCJTI*.

Au titre de la disposition traitant du principe de l'absence d'obligation légale de surveillance, les prestataires de services sont assujettis à une obligation générale de discrétion pendant la période précédant la connaissance des faits établissant l'illicéité des activités. Cette obligation générale de discrétion se matérialise par une conduite qui doit être empreinte d'indifférence face aux informations circulant ou aux activités se déroulant par le biais de leurs installations. À la différence du législateur européen qui se contente d'énoncer le principe général de l'absence d'obligation légale de surveillance, le législateur québécois se montre plus précis sur ce point en prévoyant que l'intermédiaire en question ne doit prendre aucun moyen pour empêcher les autorités responsables d'exercer leurs fonctions relativement à la sécurité publique, à la prévention, à la détection, à la preuve ou à la poursuite d'infractions[398]. Donc, c'est uniquement lorsqu'ils sont informés du caractère effectivement illicite des activités qu'ils ont l'obligation d'agir promptement afin de retirer le contenu dommageable ou de faire cesser l'activité dommageable[399]. C'est également à ce moment là qu'ils ont l'obligation de surveiller les activités afin d'empêcher toute nouvelle apparition de l'information à caractère illicite.

Hormis le cas de la réception d'une notification confirmant la présence d'activités ou d'informations illicites, la *Directive sur le commerce électronique* comporte d'autres situations qui atténuent le principe général d'absence d'obligation légale de surveillance.

La première consiste en la possibilité pour les tribunaux ou autorité administrative de contraindre les intermédiaires techniques à mettre en œuvre des mesures de prévention contre la poursuite d'activités illicites[400]. Contrairement à la loi québécoise[401] et parallèlement à la loi américaine[402], la *Directive sur le commerce*

---

[398] En vertu de l'article 27(2) de la *LCCJTI*.

[399] Le retrait de l'information ou de la cessation de l'activité doit se faire dans un délai raisonnable, à défaut de quoi il se verra opposer un éventuel recours en responsabilité sur la base de la contravention à son obligation d'agir avec promptitude. En ce sens, le temps à l'intérieur duquel il agit devient un élément important dans l'évaluation de sa responsabilité. C'est-à-dire que de son état de passiveté, l'on pourra interférer son insouciance ou aveuglement volontaire face à la commission de l'infraction. Par conséquent, la *Directive sur le commerce électronique* établit donc comme point de départ de la responsabilité la connaissance effective de l'illicéité de l'information par les prestataires de services.

[400] Ce qui est prévu aux articles 12(3), 13(3) et 14(3) de la *Directive sur le commerce électronique*.

[401] Au contraire, la loi québécoise oblige les intermédiaires techniques à ne pas empêcher les autorités responsables d'exercer leurs fonctions. Cette obligation est prévue à l'article 27(2) qui énonce ce qui suit : « Toutefois, il ne doit prendre aucun moyen pour empêcher la personne responsable de l'accès aux documents d'exercer ses fonctions, notamment en ce qui a trait à la confidentialité, ou pour empêcher les autorités responsables d'exercer leurs

électronique permet aux Parties d'exiger du prestataire de services qu'il adopte des mesures de prévention permettant de mettre un terme à la violation ou de bloquer l'accès des tiers au site contenant des informations illicites. Cette exigence peut tout aussi bien s'appliquer à un prestataire qui joue le rôle de simple transmetteur ou qui fait le stockage de l'information ou qu'à celui qui se charge de l'hébergement des données sur Internet[403]. Il est à souligner que ces mesures doivent être établies conformément aux législations internes de chacun des pays membres. Plus précisément, dans le cas du prestataire d'hébergement, la *Directive sur le commerce électronique* prévoit également pour les Parties la possibilité d'instaurer des mesures régissant le retrait de ces informations ou les actions pour en rendre l'accès impossible[404].

La deuxième réfère à l'obligation qui est mise à la charge des intermédiaires techniques *d'informer promptement les autorités publiques compétentes des activités illicites ou des informations illicites qui sont alléguées dans la notification* et pratiquées par les destinataires de leurs services dans l'environnement Internet[405]. Cette mesure ne se présente ni dans la loi québécoise et dans la loi américaine. Parallèlement à la *Directive sur le commerce électronique*, la loi française crée une même mesure tout en précisant que l'obligation d'informer avec promptitude s'applique plus spécifiquement aux activités illicites qui sont liées aux crimes contre l'humanité, à l'incitation à la haine raciale ainsi qu'à la pornographie enfantine[406]. Le législateur français se montre ainsi plus restrictif que le législateur européen.

La dernière réserve se rapporte à la mesure imposant aux prestataires techniques de *communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un contrat d'hébergement*[407]. Parallèlement à celle-ci, la loi française prévoit une mesure semblable consistant à obliger ces derniers de rendre publics les

---

fonctions, conformément à la loi, relativement à la sécurité publique ou à la prévention, à la détection, à la preuve ou à la poursuite d'infractions ».

[402] En vertu de l'article 230(d) de *Communications Decency Act*.

[403] En vertu des articles 12, 13 et 14 de la *Directive sur le commerce électronique* respectivement.

[404] En vertu de l'article 14 de la *Directive sur le commerce électronique*.

[405] En vertu de l'article 15(2) de la *Directive sur le commerce électronique*.

[406] En vertu de l'article 6-1-7 de la loi française. Ce sont les infractions visées aux cinquième et huitième alinéas de l'article 24 de la loi du 29 juillet 1881 sur la liberté de la presse et à l'article 227-23 du code pénal.

[407] En vertu de l'article 15(2) de la *Directive sur le commerce électronique*.

moyens qu'ils consacrent à la lutte contre ces activités illicites[408]. La tendance plus restrictive du législateur se maintient également dans cette mesure.

En résumé, contrairement aux principes de contrôle et de connaissance, le principe d'absence d'obligation légale de surveillance s'applique uniformément à chacun des intermédiaires, étant donné l'effort du législateur d'insérer ce principe dans la même disposition. L'on a également remarqué que les législateurs européen et français adoptent une même approche globale qui prend toutefois des ondulations au niveau des réserves s'attachant au principe. À titre d'exemple, le législateur français met en place une mesure enjoignant les intermédiaires techniques à mettre au courant les autorités compétentes sur les dispositifs et moyens qu'ils disposent en ce qui concerne les seules infractions énoncées dans le texte français alors que dans le cas du texte européen, les activités ne sont pas spécifiées en tant que telles. Par ailleurs, la *Directive sur le commerce électronique* prévoit que ce principe s'applique uniformément à l'égard des trois intermédiaires visés alors que la *LCEN* ne l'applique qu'à l'égard des deux intermédiaires[409].

En conséquence, la *Directive sur le commerce électronique*, pour asseoir un régime excluant l'obligation pour les intermédiaires d'exercer toute surveillance active précédant la réception d'une notification indiquant la présence d'informations ou activités illicites, a dû reconnaître une certaine sagesse dans leur rôle d'intermédiaires. Cette maturité s'est matérialisée tantôt par un devoir de discrétion mis à la charge des intermédiaires l'égard des activités se déroulant par le biais de leurs services, tantôt par une conduite qui soit empreinte de prudence et de diligence dès qu'ils sont tenus de retirer les informations illicites ou de faire cesser les activités illicites.

Après avoir parcouru la *Directive sur le commerce électronique*, examinons maintenant la loi française.

C) La *Loi pour la confiance dans l'économie numérique*

Dans cette section, il faut parcourir les dispositions de la *Loi pour la confiance dans l'économie numérique* (ci-après : « *LCEN* ») qui stipulent expressément le

[408] En vertu de l'article 6-1-7 de la loi française.
[409] Comme l'on verra dans le paragraphe C) visant l'étude de la loi française.

principe d'absence d'obligation légale de surveillance[410]. Au titre de ce principe, le transmetteur et l'hébergeur ne sont assujettis à aucune obligation générale de surveiller le contenu des informations qu'ils transmettent ou stockent, ni à aucune obligation générale de rechercher des faits ou des circonstances révélant des activités illicites[411]. À la différence de la *LCEN*, la *Directive sur le commerce électronique* et la loi québécoise appliquent ce principe également à l'égard de l'archiveur. Par contre, le principe général se retrouve dans la *Directive sur le commerce électronique* [412], la loi américaine[413] et la *Convention sur la cybercriminalité* ainsi que le Protocole[414]. De ce principe découle l'obligation pour ces deux intermédiaires de faire preuve de discrétion à l'égard du contenu des informations et quant à la nature des activités réalisées, sans nécessairement aller jusqu'à en devenir complètement négligent. À la différence de la loi française, la loi québécoise énonce textuellement l'obligation de faire preuve de discrétion imposée à l'encontre de ces intermédiaires[415]

Toutefois cette obligation de discrétion trouve sa limite dès qu'un titulaire de droits signale à l'intermédiaire la présence d'un contenu illicite dans une zone de stockage déterminée puisqu'à partir de ce moment, il a l'obligation de surveiller toute nouvelle apparition de ce contenu, dans n'importe quelle zone de stockage de son site. À cet égard, dans l'affaire *Google*[416], le Tribunal de commerce de Paris a estimé que *« si l'hébergeur n'est pas tenu à une obligation de surveillance générale, il est tenu à une obligation de surveillance, à partir du moment où il a eu connaissance du caractère illicite du contenu »*[417]. L'hébergeur, ayant été informé à la date du 6 octobre 2006 du caractère illicite du contenu diffusé sur son site, a agit promptement pour retirer *partiellement*

---

[410] Voir, *supra*, note 16. La *LCEN* organise un cadre juridique qui vise à promouvoir le commerce électronique, l'accroissement de la confiance dans le cyberespace et le renforcement de la sécurité des transactions électroniques, de façon à respecter les droits et libertés fondamentales. Toutefois, rappelons tout d'abord que la *LCEN* aménage le régime de responsabilité des intermédiaires techniques en fonction du rôle occupé par chacun des intermédiaires dans la chaîne de communication, à savoir le transmetteur, l'hébergeur et l'archiveur et ce, parallèlement à la *Directive sur le commerce électronique* et la loi québécoise.

[411] En vertu de l'article 6-I-7° de la *LCEN*.

[412] En vertu de l'article 15 de la *Directive sur le commerce électronique*.

[413] En vertu de l'article 230(c)(2) du *Communication Decency Act*.

[414] *Convention sur la cybercriminalité*, Rapport explicatif, *loc. cit.*, note 24, par. 105 et 119 ; *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, Rapport explicatif, *loc. cit.*, note 28, par. 25 et 45.

[415] En vertu de l'article 27(2) de la *LCCJTI*.

[416] *Google c/ Flach Films, précitée*, note 361. Dans cette décision, Flach Film et Éditions Montparnasse poursuivent *Google France* et *Google Inc* en contrefaçon pour avoir refusé de retirer efficacement les trois liens permettant d'avoir accès gratuitement au film « Le monde selon Bush » qui est diffusé dans son intégralité sur le site de Google Vidéo.

[417] *ibid.*

les liens litigieux. Toutefois, le Tribunal a précisé « *qu'à compter de cette date, il lui appartenait aussi de rendre l'accès au Film impossible* »[418]. Par conséquent, l'hébergeur devait alors effectuer une nouvelle surveillance afin de rendre l'accès au contenu litigieux impossible. Le juge a alors conclu que, n'ayant pas réalisé cette condition, l'hébergeur ne pouvait ainsi se prévaloir de la responsabilité limitée prévue par la loi.

Hormis le cas de la connaissance du caractère illicite du contenu, la *LCEN* énonce également d'autres réserves, à savoir la possibilité pour le juge de demander que soit effectuée la surveillance d'une activité, à condition qu'elle soit ciblée et temporaire[419]. Rappelons que cette mesure ne se trouve nulle part autre ni dans la loi américaine, ni dans la loi québécoise ni dans la *Convention sur la cybercriminalité*.

Comme autre réserve, la *LCEN* indique le pouvoir du juge de rendre toute ordonnance enjoignant le fournisseur de services Internet et l'hébergeur à prendre des mesures propres à prévenir la survenance d'un dommage ou à faire cesser un dommage occasionné par le contenu du service de communication qu'ils fournissent ou mettent en ligne[420]. Cette mesure de prévention permet aux intermédiaires de se protéger contre d'éventuels recours en responsabilité qui sont susceptibles de surgir à un moment donné. Et elle permet d'éviter que des dommages soient causés à des victimes du fait de la diffusion de contenus illicites. Toutefois, la tâche de circonscrire adéquatement en quoi consiste un « *dommage [potentiellement illicite]* » n'étant pas facile, il reviendra à ces intermédiaires de ne pas adopter des mesures s'avérant excessives, disproportionnées par rapport à l'objectif qui y est visé, de façon à appliquer une censure quasi-automatique sur toutes informations qui circulent par le biais de leurs services. Sur ce point, la *LCEN* se montre plus protectrice que la *Directive sur le commerce électronique* en instaurant la même mesure à l'encontre *d'un risque de violation* et non contre *une violation à la loi*. Contrairement à la loi française, la *Directive sur le commerce électronique* démontre un texte plus limpide en précisant les finalités pour lesquelles de telles mesures doivent être mises en place[421].

---

[418] *ibid.*

[419] En vertu de l'article 6-I-7° de la *LCEN*. Ronan HARDOUIN, « Observations sur les nouvelles obligations prétoriennes des hébergeurs », Juriscom.net, 08/11/2007, en ligne sur : < http://www.juriscom.net/uni/visu.php?ID=983 > (visité le 23 février 2009).

[420] En vertu de l'article 6-I-8° de la *LCEN*.

[421] La *Directive sur le commerce électronique* dispose à son article 14(3) ce qui suit : « Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation et

Enfin, la *LCEN* soulève également la nécessité pour les intermédiaires techniques d'appliquer dans certains cas une mesure qui soit proportionnelle aux dangers qu'implique la commission de crimes contre l'humanité, de l'incitation à la haine ainsi que de la pornographie juvénile afin de lutter contre la diffusion des infractions susmentionnées. À cet égard, la *LCEN* prévoit des mesures comme la mise en place de dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données[422]. Elle impose également à la charge de ces intermédiaires l'obligation, d'une part, d'informer promptement les autorités publiques compétentes de toutes activités illicites qui sont graves dès qu'elles sont portées à leur connaissance, et, d'autre part, de rendre publics les moyens qu'elles envisagent mettre de l'avant afin de lutter contre ces activités illicites[423]. Et en cas de manquement aux obligations ci-après définies, elle prévoit des sanctions pénales, notamment l'imposition d'une peine d'emprisonnement d'un an et d'une amende de 75 000 €[424]. À la différence de la *Directive sur le commerce électronique*, la *LCEN* prête à une interprétation plus restrictive de la notion d'activités illicites en circonscrivant les seules activités concernées et non pas toutes les activités ou informations illicites.

Par conséquent, le législateur français reconnaît une maturité dans le rôle des intermédiaires techniques en instituant le principe de l'absence d'obligation légale de surveillance. La sagesse législative reconnaît que ce principe ne peut être compris comme déchargeant totalement les intermédiaires de l'obligation d'effectuer toute activité de surveillance sur leurs installations et qu'il doit alors être atténué par des exceptions qui confirment la nécessité dans certaines circonstances d'effectuer une telle surveillance. Si des activités graves telles que la pornographie juvénile ou la xénophobie raciste peuvent notablement diminuer ou être résolument empêchées grâce à la mise en place, par les hébergeurs ou fournisseurs de services Internet, de moyens techniques par lesquels ils seront informés de ce qui se passe dans leurs services, le législateur se dit pourquoi ne pas imposer de telles obligations à ces derniers.

---

n'affecte pas non plus la possibilité, pour les États membres, d'instaurer des procédures régissant le retrait de ces informations ou les actions pour en rendre l'accès impossible ».

[422] En vertu de l'article 6-I-7° de la *LCEN*.

[423] En vertu de l'article 6-I-7° de la *LCEN*.

[424] En vertu des articles 6-I-7° et 6-VI-1 de la *LCEN*.

Cependant, le danger dans une telle optique est de voir les intermédiaires se substituer en de véritables « *juges* » devant se prononcer sur des situations juridiques complexes, de façon à pouvoir tracer la ligne entre la liberté de l'expression et la protection des droits fondamentaux. À cet effet, il est possible d'énoncer les propos relevés par Pascal Cohet : « *Il suffit pourtant de prendre l'exemple du site Je-boycotte-Danone. L'hébergeur avait déconnecté le site après la réaction de Danone. Mais quand le juge est intervenu, plus tard, il a estimé que le seul problème posé par le site était le détournement de logo. Autrement dit : il suffit de laisser le juge faire son travail correctement. L'intermédiaire n'en n'ayant pas les compétences. Il ne peut prendre que des décisions brutales* »[425].

Le risque de dérapage demeure toujours possible, c'est pourquoi ces mesures qui constituent une exception au principe général doivent recevoir une interprétation très restrictive et n'être appliquées qu'aux seules infractions « *graves* ». En ce qui concerne l'obligation de prendre des mesures de prévention à l'égard des activités ou informations qui sont susceptibles de se révéler illicites, la même épineuse question se pose. Sur ce, rappelons que cette disposition doit également être interprétée restrictivement et la cessation d'une activité ou le retrait d'une information ne doit alors s'effectuer que dans les cas où il existe des indices portant à conclure que l'activité est « *manifestement illicite* » et non pas uniquement « *possiblement illicite* ».

En résumé, l'on a vu que loi française énonce expressément le principe de l'absence d'obligation légale de surveillance à l'égard du transmetteur et de l'hébergeur et ce, contrairement aux lois québécoise et européenne qui l'appliquent également à l'égard de l'archiveur[426]. À la différence de la loi québécoise, la loi française ne mentionne pas expressément l'obligation de discrétion qui découle du principe de l'absence d'obligation légale de surveillance, bien qu'il s'en dégage implicitement. L'on a observé que ce principe est assorti de plusieurs réserves qui devaient être mises en place par les intermédiaires techniques afin de limiter le plus possible les risques de dérapage. L'on a constaté une rédaction plus précise de ces mesures pour la loi française qui les circonscrit aux activités les plus graves alors qu'un tel effort du législateur ne se présente ni pour la loi américaine, ni québécoise ou

---

[425] Arnaud DEVILLARD, « Le monde Internet chahute la loi sur l'économie numérique », 19 février 2003, en ligne sur : < http://www.01net.com/article/201958.html > (visité le 25 juillet 2007).

[426] Il est également possible d'appliquer ce principe à l'égard de l'archiveur sur la base du même raisonnement que celui suivi dans le paragraphe qui porte sur l'analyse du principe d'absence d'obligation légale de surveillance dans la *Convention sur la cybercriminalité*.

européenne. Par ailleurs, seul le droit français comporte des sanctions pénales ainsi que la possibilité d'exiger qu'une surveillance soit effectuée sur une activité de façon ciblée et temporaire.

En conclusion, le texte français, contrairement à la *Directive sur le commerce électronique*, comprend un principe d'absence d'obligation légale de surveillance qui est plus ciselé et plus protecteur à l'égard des tiers[427].

L'on examinera maintenant comment s'articule ce principe dans la loi américaine.

D) Le *Communications Decency Act*

Dans cette section, il faut circonscrire le principe de l'absence d'obligation légale de surveillance sous l'angle du droit américain, plus précisément du libellé l'article 230(c)(2) du *Communications Decency Act*[428]. La disposition énonce que « *[n]o provider or user of an interactive computer service shall be held liable on account of any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected* » or « *any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph* »[429]. Au titre de cette disposition, les transmetteurs et les fournisseurs d'hébergement n'ont aucune obligation de surveiller la nature des activités se déroulant par le biais de leurs installations. Toutefois, ils peuvent y procéder, de façon volontaire et en toute bonne foi, en prenant toute mesure visant à restreindre l'accès aux services qu'ils considèrent obscènes, ou trop violents et ainsi exercer une surveillance des services proposés[430]. La

---

[427] Par là, le législateur français entend souligner l'importance de punir les actes répréhensibles et graves pouvant être commis dans le cyberespace. Lorsqu'il s'agit d'actes qui sont suffisamment graves et suffisamment à blâmer pouvant justifier l'imposition de sanctions pénales, telles que les amendes, par exemple, la mise en place d'un régime de responsabilité pénale n'est pas sans utilité. Sur ce point, il faut rejoindre la « sagesse » de la position française pour affirmer que lorsqu'il s'agit de crimes tels que la pornographie juvénile et la propagande raciste et xénophobe, le découragement de tels crimes doit nécessairement passer par la mise en place d'une responsabilité pénale.

[428] *Telecommunications Act* de 1996, Pub. L. No. 104-104, tit. V, 110 Stat. 56, 133-43 (1996) (codifié dans les sections de 47 U.S.C.). Le *CDA* est situé dans le titre V du *Telecommunications Act* de 1996, qui est amendé par le *Communications Act* de 1934.

[429] Article 230(c)(2)(A)(B).

[430] L'article 230(c)(2) énonce ce qui suit : « 2) CIVIL LIABILITY- No provider or user of an interactive computer service shall be held liable on account of (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively

rédaction de cette disposition est assez concise : non seulement la loi accorde-t-elle à ces derniers un choix auquel ils ne sont pas tenus d'adhérer mais précise-t-elle également que les intermédiaires concernés n'engageront pas leur responsabilité civile ou pénale du fait de la mise en place de telles mesures de surveillances dans leurs services[431]. À la différence de la *Directive sur le commerce électronique*, des lois française et québécoise, la loi américaine n'énonce que de façon implicite ce principe et ce, parallèlement à la *Convention sur la cybercriminalité* et le Protocole.

La loi américaine renferme un cas d'exception au concept plus général de l'absence d'obligation légale de surveillance qui s'applique à un utilisateur d'un service informatique interactif, c'est-à-dire le transmetteur et le fournisseur d'hébergement. En vertu de l'article 230(d), « *[a] provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors* ». Plus loin, cette disposition stipule que « *Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections* ». Au titre de cette disposition, l'utilisateur d'un service informatique interactif doit informer son client de la présence de toute mesure de protection commercialement disponible permettant à ce dernier de limiter l'accès à des contenus ayant un caractère illicite. Cette mesure de protection permet de prévenir la survenance d'un dommage et assure une protection à l'égard des intermédiaires contre d'éventuels recours en responsabilité. À cet égard, il faut observer qu'une semblable mesure se dégageait tant de la *Directive sur le commerce électronique* que de la *LCEN*[432]. À cet égard, contrairement à loi française et à la *Directive sur le commerce électronique* qui circonscrivent le principe général en l'assortissant de plusieurs cas d'exceptions, comme le pouvoir des juges de rendre des ordonnances mises à la charge des intermédiaires visant à effectuer une surveillance sur une activité et ce, de façon ciblée

---

violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1). ».

[431] Rappelons que la loi américaine ne s'applique pas sur le plan criminel.

[432] Ce qui est prévu aux articles 12(3), 13(3) et 14(3) de la *Directive sur le commerce électronique* et l'article 6-I-8° de la *LCEN*.

et temporaire, la loi américaine, quant à elle, demeure silencieuse sur les atténuations possibles de ce principe, hormis ce cas de figure. Contrairement aux lois française et européenne qui traitent de tous les intermédiaires, à l'exception de l'intermédiaire offrant des services de référence à des documents technologiques, la loi américaine ne vise que le transmetteur et fournisseur d'hébergement. Toutefois, contrairement aux autres instruments juridiques, la loi américaine apporte une innovation sur la notion d'intermédiaire en reconnaissant la présence d'un autre intermédiaire technique, à savoir « *l'utilisateur d'un service informatique interactif* ».

En résumé, le législateur américain comprend différemment le rôle du transmetteur comparativement aux autres instruments juridiques. Selon ce dernier, l'intermédiaire, ne jouant qu'un rôle passif, doit bénéficier d'une exonération de responsabilité, pour autant qu'il n'agisse pas comme un fournisseur de contenus. Cette façon de voir du législateur américain peut en quelque sorte choquer le législateur français qui adopte une approche qui s'y oppose à plusieurs égards.

Par conséquent, la loi américaine est moins précise et moins complète que les lois québécoise, française et européenne sur ce principe, et ce, tout comme la *Convention sur la cybercriminalité*.

L'étude du principe de l'absence d'obligation légale de surveillance à travers plusieurs instruments juridiques nous apprend que le principe s'articule comme un critère d'imputabilité applicable aux intermédiaires techniques. Cette analyse nous enseigne également que ce principe comporte d'une part, le *droit* pour les intermédiaires de ne pas exercer de surveillance active sur les activités se déroulant par le biais de leurs installations et d'autre part, l'*obligation* de ne pas procéder à de telles surveillances.

Après avoir fait l'étude des principes de contrôle, de connaissance et de l'absence d'obligation légale de surveillance dans plusieurs législations, tout en faisant ressortir les différentes interprétations qu'ont données lieu ces notions auprès des tribunaux, l'on peut observer que ces principes constituent des critères permettant d'évaluer la responsabilité civile et pénale[433] des intermédiaires techniques.

---

[433] Il faut préciser que la responsabilité civile et la responsabilité pénale sont deux branches de droit qui sont totalement distinctes, ayant chacune leur logique et leurs impératifs propres. À titre d'exemple, l'absence d'intention coupable ne donnera pas lieu à une absence totale de responsabilité sur le plan civil, bien qu'il soit vrai sur le plan pénal, avec tout de même les quelques exceptions qui s'y rattachent. Pourtant, force est de constater que

Maintenant, voyons dans quelle mesure ces principes qui ressortent des normes et pratiques internationales sont conformes aux mécanismes du droit pénal canadien régissant l'imputabilité des intermédiaires techniques.

Chapitre II- L'application des principes d'imputabilité des intermédiaires techniques en droit pénal canadien

Dans le deuxième chapitre, il y a lieu d'examiner l'application des principes d'imputabilité du droit pénal canadien à l'égard de *chacun* des intermédiaires afin de savoir si le droit pénal permet d'apprécier *suffisamment* la responsabilité de chacun d'eux. Il est pertinent de traiter de cette question pour deux motifs. Premièrement, la démarche sera alors très utile afin de déterminer les conditions d'ouverture de la responsabilité pénale des intermédiaires techniques. Ce qui est en réponse à la question générale de recherche. Deuxièmement, cette question permettra de départager la responsabilité de chacun et d'orienter notre problématique de départ. Ce qui permettra de répondre à la question spécifique de recherche qui vise à savoir si les règles du droit pénal canadien régissant la responsabilité pénale des intermédiaires sont conformes aux principes qui ressortent des normes et pratiques internationales.

Dans l'étude de la mise en application des principes d'imputabilité à l'égard de *chacun* des intermédiaires, il faut se rattacher au concept de complice uniquement puisque les concepts d'auteur réel et de co-auteur ne visent que ceux qui sont à l'origine de l'activité dommageable. Or, les intermédiaires sont ceux qui ne décident *a priori* pas de l'activité dommageable. Ils ne sont alors pas assimilables à l'auteur ou au co-auteur du crime dans la mesure où ils conservent leur statut d'intermédiaires techniques. Dans ce contexte, l'on expliquera brièvement le concept de complice, étant donné qu'il est celui qui est le plus susceptible de se rapprocher de celui d'intermédiaires techniques.

Contrairement à l'auteur du crime qui en est l'auteur principal, le complice ne joue souvent qu'un rôle secondaire par rapport au crime. De la même façon, contrairement à l'éditeur qui est à l'origine de l'activité dommageable, l'intermédiaire

---

dans plusieurs législations, l'on présente les deux aspects, l'un à côté de l'autre, sans prendre la peine de faire les distinctions qui s'imposent, encore moins justifier la raison pour laquelle l'on assimile à une même chose deux réalités qui sont pourtant fort différentes.

ne participe *a priori* pas à la commission du crime. Le droit pénal canadien énonce une série de règles attribuables aux personnes complices de l'infraction. Il reconnaît deux types de complices, à savoir le complice ordinaire et le complice après le fait[434], mais le complice ordinaire est celui qui fera l'objet de notre étude[435]. Il s'agit de celui qui est animé par l'intention spécifique d'aider ou d'encourager une personne à commettre l'infraction[436]. À cet effet, le fournisseur de services Internet qui aide l'auteur du délit dans la transmission de données relatives à un code malveillant, sachant qu'elles serviront à la commission d'un acte illégal, engagera sa responsabilité à titre de complice de l'infraction[437].

Il existe une dépendance apparente entre la culpabilité du complice et le comportement de l'auteur réel. La participation de l'intermédiaire est une notion qui se situe au cœur de l'imputabilité. Il s'agit d'une notion permettant d'imputer au complice une responsabilité à partir des agissements de l'auteur réel. La culpabilité du complice n'est donc pas autonome en elle-même, elle dépend de la perpétration par l'auteur réel d'une infraction au titre du droit pénal fédéral[438]. L'illégalité du comportement de l'auteur réel a pour corollaire les trois affirmations suivantes : la complicité est impunissable a) en l'absence d'infraction sanctionnant la conduite de l'auteur réel; b) en présence d'une simple tentative de complicité et c) en l'absence de la réalisation de l'*actus reus* par l'auteur réel de l'infraction[439]. Si la culpabilité du complice est subordonnée à la réalisation par l'auteur du délit d'un fait punissable au sens du droit pénal fédéral, c'est que sa culpabilité, quant à elle, est un fait autonome

---

[434] Le complice après le fait est une personne qui apporte une aide à l'auteur principal après la commission de l'infraction. Alors que le complice ordinaire se rend coupable du même crime que l'auteur réel, le complice après le fait commet une infraction autonome : en vertu des articles 21(1), 22(1), 23 et 463 C.cr. La distinction se situe donc au niveau temporel.

[435] Puisque le complice après le fait est moins pertinent dans notre cas.

[436] *R.* c. *P. (V.L.)*, [1993] 1 R.C.S. 837, p. 790-793. Et le coauteur a) prend part personnellement à l'exécution de l'un des éléments essentiels du crime; b) agit de concert avec l'auteur réel alors que le complice : Gisèle CÔTÉ-HARPER, Pierre RAINVILLE et Jean TURGEON, « Traité de droit pénal canadien », 4e éd., Les Éditions Yvon Blais Inc., Cowansville, 1998, p. 728-731.

[437] Dans ce cas de figure, le fournisseur de services Internet ne peut être qualifié de coauteur puisqu'il ne prend pas part personnellement à l'accomplissement de l'un des éléments essentiels du crime et il n'agit pas non plus de concert avec l'auteur réel, tout ce qu'il fait, c'est de fournir une aide, celle de transmettre des données d'un code malveillant. Il ne peut non plus être qualifié de complice après le fait puisqu'il apporte une aide lors de la perpétration de l'infraction et non une fois le crime consommé.

[438] *R.* c. *Twigge (H.)*, (1996) 148 Sask. R. 254, 264-265 (C.A.) ; Gisèle CÔTÉ-HARPER, Pierre RAINVILLE et Jean TURGEON, « Traité de droit pénal canadien », *op. cit.*, note 436, p. 834.

[439] Gisèle CÔTÉ-HARPER, Pierre RAINVILLE et Jean TURGEON, « Traité de droit pénal canadien », *op. cit.*, note 436, p. 728-731, 822 et 830, 779-780 ; D. LANHAM, « Complicity, Concert and Conspiracy », [1980] 4 *Crim. L.J.* 276, p. 286.

par rapport à celle de l'auteur réel. Peu importe que la culpabilité de l'auteur réel soit reconnue ou non, ce qui importe c'est la preuve de l'illicéité du comportement de l'auteur réel[440].

Après avoir présenté la notion de complice, il convient d'apporter une précision avant d'entamer l'exercice de la mise en application des mécanismes d'imputabilité à l'égard des intermédiaires. Ainsi, le mémoire n'examinera la situation juridique de ces derniers qu'à partir du moment où la loi leur impose l'obligation d'agir[441] car le point de départ de leur responsabilité ne commence qu'à partir du moment où ils reçoivent une notification confirmant la présence d'activités illicites ou après qu'ils soient mis au courant d'une série de faits rendant apparente la commission d'activités illicites. Il serait alors inutile d'examiner leur situation juridique avant ce moment, étant donné qu'il n'existerait à ce moment-là pas de fondement sur lequel reposerait leur responsabilité pénale. C'est pourquoi l'analyse de la responsabilité pénale des intermédiaires techniques ne débutera qu'à partir du moment où ils ont une obligation légale d'agir en vertu du droit pénal canadien[442]. Et en l'absence de textes explicites énonçant cette obligation d'agir[443], il serait intéressant de voir le fonctionnement des mécanismes d'imputabilité en droit pénal canadien afin d'établir le moment à partir duquel ils ont une obligation d'agir. Dans cette perspective, il faut appliquer les règles régissant les mécanismes d'imputabilité en droit pénal canadien à chacun des intermédiaires, à savoir l'hébergeur, l'intermédiaire offrant des services de référence à des documents technologiques, l'intermédiaire qui conserve les documents à la seule fin d'assurer l'efficacité de la transmission de l'information et le transmetteur. Rappelons qu'il y a lieu de recourir à la terminologie employée dans la loi québécoise pour le simple motif que nous sommes situés sur le territoire québécois.

---

[440] Gisèle CÔTÉ-HARPER, Pierre RAINVILLE et Jean TURGEON, « Traité de droit pénal canadien », *op. cit.*, note 436, p. 836-837.

[441] Les législations des pays qui ont prévu un régime de responsabilité pénale énoncent que la responsabilité des intermédiaires ne peut être engagée tant qu'ils n'ont pas effectivement été mis au courant de l'illicéité des informations ou activités en question.

[442] L'intérêt d'examiner le régime de responsabilité des intermédiaires techniques pour les activités constituant un acte criminel au sens des lois fédérales réside dans le fait que, lorsque les crimes sont suffisamment graves et suffisamment à blâmer pour donner lieu à des sanctions pénales, le législateur pénal se doit d'intervenir afin de se conformer aux objectifs du droit pénal, à savoir sa fonction répressive, protectrice et expressive. Toutefois, il faut souligner que le législateur ne doit intervenir que lorsque le crime possède un niveau gravité suffisant et les dispositions des infractions ainsi légiférées doivent recevoir une interprétation restrictive.

[443] Précisons que cette obligation d'agir existe par contre dans le droit pénal provincial par le biais de la *LCCTJI*.

a) L'hébergeur

Dans ce premier paragraphe, il convient d'étudier les mécanismes d'imputabilité du droit pénal canadien qui régissent l'hébergeur[444]. Plus précisément, le mémoire analysera la notion de complicité qui est un mode de participation à la commission de toute infraction criminelle puisqu'il s'agit du seul concept qui se trouve directement applicable à l'hébergeur[445].

L'hébergeur agit à titre de complice[446] lorsqu'il *accomplit ou omet d'accomplir quelque chose en vue d'aider ou d'encourager* l'auteur réel dans la commission du crime[447]. L'*actus reus* de l'article 21 C.cr. découlera alors de la conduite de l'hébergeur, selon son niveau de participation à l'activité en question. Il peut s'agir d'un cas où il accomplit un acte positif. Ainsi, le fournisseur de services Internet qui donne l'accès à ses services, sachant que l'internaute s'apprête à commettre une fraude, sera qualifié de complice. Comme autre exemple, prenons le cas où un blogueur encourage l'usager à poster des messages à caractère raciste ou xénophobe sur son blogue. Par ailleurs, l'hébergeur peut agir en tant que complice lorsqu'il omet d'accomplir quelque chose. Ainsi, si l'hébergeur a le pouvoir d'empêcher la poursuite d'une activité qu'il sait être illégale et qu'il ne fait rien pour l'en empêcher, il pourra alors recevoir la qualification de complice puisque son omission d'agir permet d'aider ou d'encourager la commission du crime. C'est notamment le cas lorsqu'il n'agit pas promptement pour retirer l'information litigieuse ou pour en rendre l'accès impossible dès qu'il est mis au courant de la présence d'activités illicites par le biais de ses installations.

---

[444] Il s'agit de celui qui agit pour offrir des services de conservation de documents technologiques sur un réseau de communication et qui met des documents appartenant à des tiers à la disposition du public par le biais de ses services. Son rôle est comparable à celui du propriétaire des lieux puisqu'il n'est pas responsable tant qu'il n'a pas de fait connaissance des activités illicites se déroulant par le biais de ses services.

[445] En vertu de l'article 21(b) et 21(c) qui se lisent comme suit : « **21.** (1) Participent à une infraction : [...] *b*) quiconque accomplit ou omet d'accomplir quelque chose en vue d'aider quelqu'un à la commettre; *c*) quiconque encourage quelqu'un à la commettre.

[446] Toutefois, il convient de préciser que l'hébergeur qui exerce un niveau de contrôle tel qu'il lui permet de réaliser l'une des composantes essentielles de l'infraction pourra être qualifié d'auteur réel ou de coauteur, s'il y a multiplicité d'acteurs dans la commission du crime. Ainsi, l'hébergeur qui est à l'origine de la transmission ou qui modifie le contenu de l'information ou le cours de traitement des données aura participé à un élément constitutif de l'infraction et sera alors considéré comme l'auteur réel de l'infraction. Si l'hébergeur est celui qui tient les propos haineux ou celui qui modifie le contenu du message de façon à inclure des propos haineux, c'est qu'il n'est plus un simple intermédiaire mais un auteur réel de l'infraction, plus précisément l'auteur matériel.

[447] Ce qui équivaut à l'*actus reus* de l'infraction édictée à l'article 21 C.cr.

Dans l'environnement électronique, les agissements de l'hébergeur peuvent également permettre de déceler la *mens rea* de l'article 21 C.cr. qui se rattache à l'*intention d'aider ou d'encourager la commission du crime*[448]. Il est possible de déceler l'élément mental de l'infraction en se servant des concepts de la connaissance et de l'intention[449]. Il convient d'expliquer brièvement en quoi consistent ces deux concepts afin de mieux comprendre le moment à partir duquel cet intermédiaire a l'obligation d'agir. Tout d'abord, la notion de connaissance qui se situe au cœur de la *mens rea* de la faute subjective peut exister sous trois formes, à savoir la *connaissance réelle*[450], *l'ignorance volontaire*[451] et la *connaissance présumée*[452]. Ensuite, le concept de l'intention détermine l'état d'esprit de l'accusé lors de la commission du crime[453]. Il est possible de faire un rapprochement entre ces deux concepts qui font partie d'un même ensemble, à savoir l'élément mental de l'infraction. Rappelons que l'on avait

---

[448] Voir à cet égard : *R.* c. *Greyeyes*, [1997] 2 R.C.S. 825, 8 C.R. (5th) 308, 116 C.C.C. (3d) 334.

[449] Gisèle CÔTÉ-HARPER, Pierre RAINVILLE et Jean TURGEON, « Traité de droit pénal canadien », *op. cit.*, note 436, p. 263.

[450] La *connaissance réelle ou factuelle* désigne la connaissance qu'a l'accusé sur les faits et les circonstances qui constituent l'acte criminel. Ainsi, la *mens rea* réside dans le fait de la commission de l'acte criminel par l'accusé en ayant connaissance des éléments constitutifs de l'infraction. Hugues PARENT, « Traité de droit criminel », 2e éd., Les Éditions Thémis, Montréal, 2007, p. 79.

[451] L'*ignorance volontaire* correspond à un état d'esprit qui choisit délibérément de rester dans l'ignorance des faits ou des éléments constitutifs de l'infraction alors qu'il pouvait se renseigner : Hugues PARENT, « Traité de droit criminel », *op. cit.*, note 450, p. 80; Gisèle CÔTÉ-HARPER, Pierre RAINVILLE et Jean TURGEON, « Traité de droit pénal canadien », *op. cit.*, note 436, p. 388 : « La personne a eu des soupçons, a réalisé la probabilité de l'existence d'un fait ou d'une circonstance, mais a préféré ne pas obtenir une confirmation pour pouvoir par la suite nier la connaissance ».

[452] La *connaissance imputée* consiste à « *impute[r] à l'accusé, qui ignore un fait ou une circonstance de l'infraction, la connaissance de ce fait ou circonstance lorsque la personne raisonnable et prudente aurait été au courant de ce fait* », sachant que la loi l'imposait l'obligation de se renseigner : Gisèle CÔTÉ-HARPER, Pierre RAINVILLE et Jean TURGEON, « Traité de droit pénal canadien », *op. cit.*, note 436, p. 396. À la différence de l'aveuglement volontaire où l'accusé pouvait se renseigner et ne l'a pas fait, dans le cas de la connaissance imputée, l'accusé pouvait et devait se renseigner alors qu'il a délibérément omis de le faire.

[453] L'intention (du latin : *intendere*, qui signifie « tendre vers ») désigne un acte de volonté qui est dicté suivant l'ordre de la raison sur la base de la connaissance de l'objet vers lequel la raison ordonne la volonté de mouvoir : Hugues PARENT, « Traité de droit criminel », *op. cit.*, note 450, p. 155; SAINT AUGUSTIN, *Retract.* I, 9. PL 32, 596. BA 12, 319, cité dans Thomas D'AQUIN, *Somme théologique*, t. 2, Paris, Éditions du Cerf 1997, quest. 12, art. 1, p. 99. Une autre formulation de la définition de l'intention apparaît comme la suivante : « *[u]ne personne vise intentionnellement un événement si elle a pour but conscient de causer l'événement. Une personne vise aussi intentionnellement l'événement lorsqu'elle n'a ni l'intention ni pour objectif de causer l'événement, mais prévoit que l'événement (la conséquence) résultera certainement ou presque certainement de l'acte qu'elle accomplit pour atteindre un autre but. Dans ce dernier cas, la personne est présumée avoir visé intentionnellement la conséquence inévitable de son acte, indépendamment de son but véritable* » : *R.* c. *Chartrand*, [1994] 2 R.C.S.864, 983-984 ; Gisèle CÔTÉ-HARPER, Pierre RAINVILLE et Jean TURGEON, « Traité de droit pénal canadien », *op. cit.*, note 436, p. 436. Dans cette définition, la juge l'Heureux-Dubé distingue un acte intentionnel et volontaire d'un acte intentionnel et non volontaire. Dans les deux cas, la conséquence de l'acte est voulue dans le sens de l'acception juridique du terme de l'intention. L'acte est par contre involontaire lorsque la conséquence qui découle de l'acte est obtenue à la suite non pas d'un choix réel exercé par l'individu mais d'un choix dicté par « *les instincts normaux de l'être humain* » : *R.* c. *Perka*, [1984] 2 R.C.S. 232. Il s'agit d'un acte involontaire au point de vue normatif ou moral. C'est pourquoi l'intention exclut les actes qui sont commis par automatisme, ignorance, erreur et contrainte physique : Hugues PARENT, « Traité de droit criminel », *op. cit.*, note 450, p. 158.

fait un tel rapprochement en analysant la connaissance dans la *Convention sur la cybercriminalité*, à la lumière des commentaires formulés dans le rapport explicatif de la Convention et du Protocole[454]. Ainsi, l'on présumera que l'hébergeur qui *aide ou encourage l'auteur réel* dans la commission du crime ou celui qui le commet réellement a visé intentionnellement la conséquence inévitable de son acte puisqu'il prévoyait que l'événement (la conséquence) résulterait certainement ou presque certainement de l'acte qu'il a accomplit, peu importe qu'il ait l'intention ou non de causer l'événement[455]. Ce qui implique la connaissance du caractère illicite de l'activité en question. À titre d'exemple, si le blogueur encourage la vente d'objets nazis sur son site Web, malgré qu'il soit mis au courant du caractère illicite de l'activité, on peut penser qu'il prévoit que l'événement –c'est-à-dire, la vente d'objets nazis– résultera certainement de l'acte qu'il accomplit, c'est-à-dire permettre l'accès à son site Web malgré la connaissance de la situation illégale.

Il est possible d'imputer à l'hébergeur la connaissance du caractère illégal d'une activité en se servant de la dynamique découlant des notions de la i) faute subjective, laquelle comporte trois composantes, à savoir a) la connaissance (*la connaissance réelle, l'ignorance volontaire et la connaissance présumée*), b) l'intention et c) l'insouciance, ii) des notions de l'*actus reus* et iii) de la *mens rea.* Il est important de déterminer si l'hébergeur avait connaissance du caractère illicite de l'activité puisque son obligation d'agir commence à ce moment-là. Ainsi, il est possible d'imputer la connaissance de l'illicéité de l'activité se déroulant par le biais de ses services en se servant de cette dynamique. À titre d'exemple, le fait pour ce dernier de recevoir une notification confirmant la présence d'activités illicites dans ses installations et d'obtenir, par la suite, la confirmation de l'illicéité de cette activité auprès d'un tiers indépendant permettra de lui imputer une *connaissance réelle* du caractère litigieux d'une activité[456]. Comme autre exemple, l'hébergeur qui reçoit une notification indiquant la présence d'activités illégales par le biais de son site Web et qui, par la suite, omet de s'adresser à un tiers indépendant pour qu'il puisse confirmer

---

[454] *Convention sur la cybercriminalité*, Rapport explicatif, *loc. cit.*, note 24, par. 105 ; *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, Rapport explicatif, *loc. cit.*, note 28, par. 25

[455] Ce qui réfère à un acte intentionnel volontaire ainsi qu'à un acte intentionnel non volontaire.

[456] Par exemple, la procédure rigoureuse de notification prévue à l'article 6-I-5 de la *LCEN*.

ou infirmer la véracité de cette allégation aura également l'obligation d'agir, étant donné qu'il a une *connaissance imputée* de la situation. Dans ce cas de figure, non seulement l'hébergeur « *peut* » savoir mais « *doit* » savoir. Enfin, cette obligation pourra également naître d'une série de faits rendant apparente la commission d'activités illicites, ce qui équivaudra à de l'insouciance, si l'hébergeur, sachant qu'il « *peut* » et « *doit* » agir, s'abstient de le faire[457].

Après avoir fait l'analyse de ce qui précède, il y a lieu de faire le constat suivant : le droit pénal canadien ne comporte qu'une seule disposition qui s'applique directement à l'hébergeur, à savoir celle visée à l'article 21 C.cr. Il faut observer que les alinéas b) et c) de cette disposition ne viennent que définir en quoi consiste la notion de complicité, ne distinguant pas outre mesure ce qui advient de l'hébergeur, en comparaison avec les autres intermédiaires. Le droit pénal général ne reconnaît en fait que deux types d'« *intermédiaires* » : le complice ordinaire et le complice après le fait. L'hébergeur fait partie de la première catégorie de complice. Qu'en est-il de l'intermédiaire offrant des services de référence à des documents technologiques?

b) L'intermédiaire offrant des services de référence à des documents technologiques

Dans ce deuxième paragraphe, il faut étudier les règles d'imputabilité visant l'intermédiaire qui offre des services de référence à des documents technologiques, à savoir un index, des hyperliens, des répertoires ou des outils de recherche.

Les services de référencement s'effectuent par le biais de moteurs de recherche. Selon l'Office de la langue française, un moteur de recherche est un « *[p]rogramme qui indexe le contenu de différentes ressources Internet, plus particulièrement de sites Web, et qui permet, à l'aide d'un navigateur Web, de rechercher de l'information selon différents paramètres, en se servant de mots-clés, ou par des requêtes en texte libre, et d'avoir accès à l'information ainsi* trouvée »[458]. Il s'agit ainsi d'un mécanisme qui fournit un service d'indexation afin de retrouver les documents se rattachant aux critères de la requête que l'on effectue sur le site du moteur de recherche.

---

[457] Il s'agira de l'aveuglement volontaire, si l'hébergeur choisit de ne pas se renseigner alors qu'il pouvait le faire, malgré qu'il soit mis au courant d'une série de faits qui prennent la forme de simples soupçons.

[458] Office québécois de la langue française, *Le grand dictionnaire terminologique*, Recherche –moteur de recherche, en ligne sur : < http://www.granddictionnaire.com > (visité le 27 janvier 2009).

L'on compte les annuaires ou répertoires de recherche comme autres types d'outils de recherche. Un répertoire de recherche est un système de classification de données regroupant les données dans des catégories distinctes qui sont répertoriés sur un support de stockage, de manière à faciliter la consultation des données. Contrairement au moteur de recherche, un répertoire de recherche ne référencera pas l'adresse URL de façon automatique puisqu'il n'utilise pas de logiciel d'indexation[459].

La situation juridique de cet intermédiaire est particulière en raison de son mode de fonctionnement. Comme le rôle de ces outils de recherche ne consistent qu'à fournir un service de référencement ou d'indexation automatique des sites Web afin de faciliter le repérage de l'information, il serait alors difficile de prétendre que cet intermédiaire pourrait agir en tant que complice aux termes de la disposition visant l'article 21 Ccr. Puisque celui qui distribue de l'information dans un système de référencement de données tel qu'un bibliothécaire ne maîtrise pas le contenu de l'information et n'est pas au courant du caractère illicite de son contenu.

Comme il est difficile de voir comment l'on pourrait établir l'*actus reus* et la *mens rea* de l'infraction visée à l'article 21 Ccr., cet intermédiaire ne peut alors être assimilable à titre de complice[460]. Puisque le fait de rendre disponible sur un répertoire de l'information ne pourrait relever d'un acte qui est de la nature à « *aider ou encourager* » l'auteur réel de l'infraction. Prenons l'exemple le plus courant du lien qui réfère à un site contenant de la pornographie juvénile. Ainsi, le moteur de recherche n'apporte pas d'*aide* à une personne qui « *produit ou vend* » du matériel contenant un matériel explicite puisque le site Web était déjà existant avant que *Google* ne le regroupe sur un répertoire de données. Le moteur de recherche n'a fait que reprendre ce site Web et le placer sous un répertoire selon des critères prédéterminés.

---

[459] Office québécois de la langue française, *Le grand dictionnaire terminologique*, Recherche –répertoire de recherche, en ligne sur : < http://www.granddictionnaire.com > (visité le 27 janvier 2009) : « *Il faudra donc donner plus de renseignements qu'une simple URL (le titre, un texte descriptif, une catégorie et quelques mots-clés), afin qu'il référence le site dans la catégorie la plus appropriée. Yahoo, Nomade et La Toile du Québec sont des exemples de répertoires* ».

[460] Il n'est pas nécessaire d'aborder la question de savoir si l'intermédiaire offrant des services de référencement à un site Web peut être qualifié à titre d'auteur réel. Puisque celui qui héberge un site Web à des fins de distribution de matériels à contenus explicites a déjà commis le crime s'y reliant avant même qu'il est consulté Google afin de retrouver le site Web. En ce sens, le moteur de recherche ne contribue en rien à la réalisation du crime en question.

En résumé, les mécanismes d'imputabilité ne permettent pas d'apprécier *pleinement* la responsabilité pénale de l'intermédiaire offrant des services de référence à des documents technologiques. Le droit pénal canadien ne comporte pas de mécanisme d'imputabilité permettant de lui imputer une responsabilité pénale puisque la qualification de complice ordinaire ne s'applique nullement à cet intermédiaire. Qu'en est-il de l'intermédiaire qui conserve les documents à la seule fin d'assurer l'efficacité de leur transmission ultérieure?

c) L'intermédiaire qui conserve les documents à la seule fin d'assurer l'efficacité de leur transmission ultérieure

Dans ce troisième paragraphe, il faut étudier l'intermédiaire qui conserve les documents à la seule fin d'assurer l'efficacité de leur transmission ultérieure[461]. La situation juridique de cet intermédiaire est assimilable à celle de complice ordinaire[462] en raison de la nature de ses fonctions.

L'intermédiaire en question agit à titre de complice ordinaire lorsqu'il pose des gestes ou omet de poser des gestes qui sont de nature *à aider ou encourager l'auteur du crime* dans la réalisation du crime[463]. Ainsi, l'intermédiaire peut être tenu responsable à titre de complice lorsqu'il *pose des actes positifs en vue d'aider ou d'encourager l'auteur réel* dans la réalisation de l'infraction. À titre d'exemple, le fait de sélectionner la personne qui transmet le document, le reçoit ou qui y a accès ou de conserver le document plus longtemps que nécessaire pour sa transmission agit à titre de complice. Par ailleurs, l'on peut imputer une responsabilité à l'intermédiaire qui *omet de poser des actes* dans le but *d'aider ou d'encourager l'auteur réel* dans la commission de l'infraction. À titre d'exemple, l'intermédiaire qui omet de retirer promptement du réseau le document ou ne rend pas l'accès au document impossible alors qu'il a de fait connaissance du caractère illicite des activités se déroulant par le

---

[461] Il peut s'agir d'un serveur à accès contrôlé, d'un hébergeur pour des documents destinés à des personnes spécifiquement désignées ou bien encore d'un prestataire offrant un service d'intranet La conservation de documents peut s'effectuer par un procédé d'antémémorisation qui permet le stockage des éléments d'une page Web dans un serveur, de manière à accéder plus facilement à ladite page Web. Ce procédé peut être pratiqué autant par les exploitants des réseaux, autant par les usagers que par les proxies qui sont des intermédiaires entre le navigateur de l'usager et le serveur Web. Et les opérateurs du réseau pratiquent l'antémémorisation des sites Web en stockant sur le serveur *proxy* les documents les plus fréquemment consultés afin d'en faciliter l'accès.

[462] En vertu des alinéas b) et c) de l'article 21 C.cr.

[463] *ibid.*

biais de ses installations sera assujetti à la responsabilité découlant du statut de complice.

Quant au moment à partir duquel il a l'obligation d'agir, il faut se référer aux commentaires formulés concernant l'hébergeur qui se trouvent également applicables pour ce dernier[464].

En résumé, le droit pénal canadien applique le même statut de complice ordinaire tant à l'égard de cet intermédiaire qu'à l'égard de l'hébergeur. Contrairement aux instruments juridiques nationaux et internationaux analysés précédemment[465] qui soulèvent des distinctions entre ces deux intermédiaires, le droit pénal canadien, quant à lui, assimile ces deux intermédiaires au même concept de complice. Par conséquent, le droit pénal canadien ne permet pas de situer *spécifiquement* la responsabilité imputable à cet intermédiaire, étant donné qu'il est assujetti à une même situation juridique que l'hébergeur.

Qu'en est-il du transmetteur?

d) Le transmetteur

Dans ce dernier paragraphe, il faut examiner l'application des mécanismes d'imputabilité du droit pénal à l'endroit du transmetteur[466]. La situation juridique du transmetteur est comparable à celle de complice de l'infraction puisque dans les deux cas, ils prennent un rôle secondaire dans la réalisation du crime[467].

Le transmetteur est assujetti aux alinéas b) et c) de l'article 21 C.cr. qui définit les participants à une infraction, notamment le complice. En vertu de ces alinéas, le

---

[464] Voir p. 115.

[465] L'on peut soulever des rapprochements entre cet intermédiaire et le transmetteur lors de l'analyse des législations se présentant dans le chapitre I de la partie II. Cet intermédiaire, tout comme le transmetteur, ne maîtrisent aucunement l'information qu'ils possèdent et ne sont pas *a priori* au courant du contenu de l'information. Ces deux intermédiaires n'ont pas la capacité de vérifier le contenu de l'information ou activité en question. Rappelons toutefois la nuance qui est à l'effet que le transmetteur exerce un plus grand contrôle qu'un intermédiaire qui conserve les documents à la seule fin d'assurer l'efficacité de la transmission.

[466] Il s'agit de celui qui exerce le rôle d'un simple transporteur d'informations. Il sert de conduit pour transporter de l'information du point de départ de l'expédition du document jusqu'à son point d'arrivée. De par sa définition même, le transmetteur n'assume aucun rôle actif dans la chaîne de communication électronique puisqu'il a l'obligation de transporter sans discrimination le contenu de l'information. En règle générale, il ne peut lui être reproché d'avoir participé à l'activité illicite lorsqu'il ne sert que de simple conduit au transport de l'information et compte tenu des limites de sa capacité à apprécier l'illégalité, l'illicéité ou le caractère dommageable de son contenu. Il ne pourra *a prime abord* recevoir ni la qualification d'auteur réel ni celle de complice. Puisque le fait de transporter de l'information n'équivaut pas à « *aider ou encourager* » l'auteur réel dans la perpétration de l'un des éléments essentiels du crime.

[467] En vertu des alinéas b) et c) de l'article 21 C.cr. Voir à cet égard les pages 108 et 109.

transmetteur *qui pose ou omet de poser des actes qui sont de nature à aider ou à encourager l'auteur du crime* dans la réalisation du crime est qualifié de complice ordinaire[468]. Ainsi, le transmetteur agira à titre de complice lorsqu'il se comporte de manière à contribuer à la réalisation du crime, soit en *posant un acte positif* ou un *acte d'omission*. Ainsi, seront attribuables au complice les actes qui consistent à sélectionner le destinataire du service, à fournir un procédé automatique de stockage ou de transmission des données ou à maintenir les informations stockées pendant une durée excédant le temps raisonnablement requis pour assurer le stockage ou la transmission de données ou le fait de ne pas supprimer le lien litigieux une fois mise au courant du caractère illicite de l'information en question.

En résumé, le transmetteur obéit aux mêmes règles de complicité que l'hébergeur ainsi que l'intermédiaire qui conserve les documents à la seule fin d'assurer l'efficacité de la transmission ultérieure de l'information. Le transmetteur se voit imputer le rôle de complice ordinaire, tout comme les autres intermédiaires, à l'exception de l'intermédiaire offrant des services de référence à des documents technologiques.

Après avoir appliqué les principes d'imputabilité à l'endroit de chacun des intermédiaires techniques, l'on peut constater qu'ils permettent de situer *très largement* la responsabilité imputable à ces derniers. Le concept de complice est d'une certaine utilité pour évaluer leur responsabilité pénale. Toutefois, ce concept trouve vite sa limite lorsque l'on l'applique à *chacun* des intermédiaires et ce, de façon isolée. Puisque le droit pénal ne prévoit qu'un seul type de participant à l'infraction qui puisse être applicable aux intermédiaires techniques, à savoir le complice ordinaire. Lorsque l'on rattache ce concept à chacun des intervenants électroniques, il s'ensuit que le même rôle de complice ordinaire se retrouve à la fois applicable pour l'hébergeur, pour l'intermédiaire qui conserve les documents à la seule fin d'assurer l'efficacité de leur transmission ultérieure, que pour le transmetteur. Or, le rôle de l'hébergeur se distingue à plusieurs égards de celui du transmetteur ou de l'archiveur. C'est d'ailleurs ce que révèle l'état du droit dans les différentes législations examinées dans le Titre I. Par ailleurs, le droit pénal ne comporte pas de mécanisme d'imputabilité régissant la

[468] Voir à ce sujet les pages 110 et 111.

responsabilité de l'intermédiaire offrant des services de référence à des documents technologiques.

CONCLUSION

L'examen des instruments juridiques nationaux et internationaux mentionnés dans le titre I révèle que les principes de contrôle, de connaissance et de l'absence d'obligation légale de surveillance apparaissent comme des principes directeurs se reliant à l'imputation de responsabilité des intermédiaires techniques. Si l'intervenant n'exerce aucun contrôle sur l'information ou activité en question, il bénéficiera alors d'un régime d'exonération de responsabilité. De la même façon, s'il n'est pas au courant de l'activité ou information en question, il ne sera pas tenu d'agir en vertu de la loi. D'ailleurs, si la loi ne lui impose pas d'obligation légale de surveillance, il ne sera pas présumé connaître le contenu des informations transitant par le biais de ses installations ou des activités s'y déroulant. Par conséquent, ces trois critères doivent être compris comme des principes d'imputabilité permettant d'apprécier la responsabilité des intermédiaires techniques.

Qu'en est-il des mécanismes d'imputabilité du droit pénal canadien? Permettent-ils d'apprécier suffisamment la responsabilité de *chacun* des intermédiaires? Quelles sont les conditions d'ouverture de la responsabilité de chacun d'eux? Ce sont là toutes les questions auxquelles ce mémoire a répondu dans sa partie II.

L'analyse du fonctionnement des mécanismes du droit pénal canadien à l'égard de chacun des intermédiaires techniques a permis de faire les constatations suivantes. Seul le concept de complice ordinaire permet d'imputer une responsabilité à l'encontre des intermédiaires techniques, à l'exception de l'intermédiaire offrant des services de référence aux documents technologiques. Ainsi, les intermédiaires techniques (à l'exception de l'intermédiaire offrant des services de référence aux documents technologiques) ne peuvent être alors tenus responsables qu'en vertu de l'article 21 C.cr. Pour engager leur responsabilité pénale, ces derniers[469] doivent remplir les deux conditions suivantes. Tout d'abord, ils doivent se comporter de manière *à aider ou*

[469] Toujours à l'exception de l'intermédiaire offrant des services de référence aux documents technologiques.

encourager l'auteur du crime dans la réalisation de l'activité en question[470]. Ensuite, ils doivent avoir *l'intention d'aider ou d'encourager* l'auteur réel dans la commission du crime[471]. Ce qui est en réponse à la question générale de recherche qui vise à déterminer les conditions d'ouverture de la responsabilité de chacun des intermédiaires techniques.

En ce qui concerne la question spécifique de recherche, nous entretenons des doutes quant à la conformité des mécanismes du droit pénal canadien régissant la responsabilité pénale des intermédiaires techniques aux principes (de contrôle, de connaissance et d'absence d'obligation légale de surveillance) ressortant des normes et pratiques internationales. Puisque les mécanismes d'imputabilité, tels qu'ils existent en droit pénal canadien, ne sont pas suffisamment précis au point de permettre une appréciation *complète* de la responsabilité à l'égard de *chacun* des intermédiaires techniques. Le droit pénal canadien se contente d'énoncer une série de règles qui sont d'application *uniformes* à l'égard de *tous les intermédiaires techniques*, sans pour autant délimiter précisément ce qui adviendra de l'hébergeur en comparaison avec le transmetteur et l'intermédiaire qui assume le rôle de la conservation de documents. Or, le rôle assumé par l'hébergeur se distingue à plusieurs égards avec celui du transmetteur et de celui de l'archiveur. C'est d'ailleurs le constat qui ressort lorsque l'on a rattaché le concept de complice à chacun des intermédiaires. Ces règles n'établissent pas de réelles distinctions entre chacun des intermédiaires, se contentant de régler la question de la responsabilité pénale des intermédiaires en assimilant chacun d'eux au statut de complice. Par ailleurs, le droit pénal canadien, tel qu'il existe actuellement, ne permet pas d'imputer une responsabilité au moteur de recherche.

Dans cette perspective, il est possible de se poser la question de savoir quelles sont les mesures qui doivent être mises en œuvre par le Canada afin de rendre sa législation interne conforme aux principes ressortant des pratiques et normes internationales en matière de responsabilité des intermédiaires techniques?

Nous suggérons au législateur pénal de prendre des mesures nécessaires afin d'apporter les modifications requises au *Code criminel* en vue de rendre sa législation

---

[470] Ce qui se rapporte à l'*actus reus* de l'infraction.
[471] Voir à cet égard : *R.* c. *Greyeyes*, *précitée*, note 448. Ce qui correspond à la *mens rea* de l'infraction.

interne conforme aux principes ressortant des normes et pratiques internationales[472]. Toutefois, il faut tout d'abord étudier plus à fond les effets économiques de ce changement législatif à l'aide d'une analyse économique du droit et implanter un processus de consultation[473] auprès de divers intervenants afin de tenir compte de toutes les conséquences probables qu'implique ce choix législatif. Les nouvelles dispositions législatives doivent répondre aux objectifs suivants : a) elles doivent être adaptées aux nouvelles technologies de l'information ; b) elles doivent prévoir la responsabilité imputable à *chacun* des intermédiaires techniques et être établies dans des circonstances bien délimitées[474].

Une fois que les modifications législatives proposées auront été adoptées, il sera alors possible de conclure à la conformité du droit pénal aux principes ressortant des normes et pratiques internationales. En ce qui concerne la *Convention sur la cybercriminalité* ainsi que le *Protocole*[475], il faudra attendre leur ratification éventuelle par le Canada[476]. Si une telle ratification advient, nous pourrons, sur la base d'un principe interprétatif[477], présumer alors la conformité du droit pénal canadien à ces deux textes internationaux. Autrement dit, en vertu de ce principe, nous pourrons

---

[472] C'est-à-dire les instruments juridiques nationaux et internationaux étudiés dans le chapitre I du titre II: *Convention sur la cybercriminalité*, STE n° : 185, Budapest, 23 novembre 2001 et *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, STE n°: 185, Strasbourg, 28 janvier 2003 ; Directive *2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur*, *supra*, note 15; *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, *supra*, note 16; *Loi concernant le cadre juridique des technologies de l'information*, *supra*, note 7 et *Communications Decency Act*, *supra*, note 18.

[473] Le processus de consultation qui porte sur l'accès légal a déjà été fait par les intervenants concernés. Dans le cadre de cette consultation, l'on visait à : « mettre à jour [l]a législation [canadienne] en matière d'accès légal afin d'être en mesure de ratifier la *Convention sur la cybercriminalité* et d'honorer ses engagements internationaux, notamment envers les États du G8 » : Ministère de la Justice du Canada, « Résumés des mémoires présentés dans le cadre de la consultation sur l'accès légal », 6 août 2003, en ligne sur : < http://www.justice.gc.ca/fra/cons/al-la/res-sum/index.html > (visité le 19 mars 2009).

[474] Les sanctions doivent être proportionnelles à la gravité du crime commis, notamment par le biais d'amendes d'un montant considérable ou par le biais de la mise en place d'une liste sur laquelle figure les intermédiaires qui ont contrevenu à la loi. Lorsque le comportement est suffisamment à blâmer et suffisamment odieux, il revient au législateur pénal de créer des dispositions incriminant le comportement par le biais de sanctions efficaces afin d'assurer les fonctions expressives, répressives et protectrices du droit pénal canadien.

[475] *Convention sur la cybercriminalité*, STE n° : 185, Budapest, 23 novembre 2001 et *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, STE n°: 185, Strasbourg, 28 janvier 2003.

[476] Le Canada n'a pas ratifié à l'heure actuelle ces deux instruments internationaux.

[477] Il s'agit de la présomption de conformité du droit interne canadien à ses obligations internationales. Voir à cet égard : Rebecca J. COOK et Lisa M. KELLY, « La polygynie et les obligations du Canada en vertu du droit international en matière de droits de la personne », Ottawa, Canada, Section de la famille, des enfants et des adolescents, ministère de la Justice du Canada, septembre 2006, en ligne sur : < http://www.justice.gc.ca/fra/min-dept/pub/poly/index.html#01 > (visité le 18 mars 2009) ; G. van Ert, « Using international law in Canadian courts » 2002 *Kluwer Law International*, p. 99-100.

inférer la volonté du législateur pénal canadien d'être conforme aux normes découlant des ces deux textes internationaux, à partir de leur ratification éventuelle par le Canada[478]. À cet égard, les tribunaux canadiens ont d'ailleurs reconnu et appliqué cette présomption de conformité à maintes reprises[479].

Toutefois, à l'heure actuelle, il est difficile de conclure fermement que le droit pénal canadien est conforme aux normes découlant des normes et pratiques internationales en matière de responsabilité pénale des intermédiaires techniques. Par conséquent, il est pressant pour les juristes de se pencher sur la question de la responsabilité pénale de ces intermédiaires et d'entamer un travail sérieux de réflexion sur la solution proposée dans ce mémoire, à savoir la possibilité de créer dans le *Code criminel* des dispositions régissant spécifiquement la responsabilité imputable à *chacun* des intermédiaires.

---

[478] Il faut toutefois préciser que cette présomption est réfutable, à condition d'avoir dans le libellé de la loi une énonciation expresse qui indique « *l'intention non équivoque du législateur de manquer à une obligation internationale* » : *R.* c. *Hape*, [2007] 2 R.C.S. 292, 2007 CSC 26.
Les auteurs Keyes et Sullivan mentionnent ce qui suit à propos de cette présomption : « *Il y a enfin la présomption de conformité avec le droit international. Compte tenu des formulations courantes de la présomption, on doit tenir pour acquis qu'elle s'applique à toutes les obligations imposées au Canada par le droit international, sans égard à la source — droit coutumier ou convention — et, s'agissant d'une convention, que cette dernière ait été mise en œuvre ou non. Évidemment, la convention qui n'a pas été ratifiée n'entraîne aucune obligation, mais une fois ratifiée, elle a force obligatoire pour le Canada, peu importe qu'elle ait été mise en œuvre ou non* [J'ai souligné]» : John Mark KEYES et Ruth SULLIVAN, « A Legislative Perspective on the Interaction of International and Domestic Law », dans Oonagh E. Fitzgerald et al, *The Globalized Rule of Law*, Éditions Irwin Law, 2006, en ligne sur : < http://www.ciaj-icaj.ca/english/publications/124Keyes-Sullivan%20_version%20francais_.pdf > (visité le 18 mars 2009).
Précisons que la présomption de conformité se fonde sur la prémisse selon laquelle les tribunaux sont tenus d'éviter une interprétation du droit interne qui irait à l'encontre des obligations internationales de l'État, sauf en cas d'indications contraires dans le libellé de la loi. Ce qui suppose que le tribunal doit éviter de choisir une interprétation qui engagerait la violation de ses obligations. À cet égard, l'auteur Sullivan explique que cette présomption comporte deux volets. Le premier volet est à l'effet que l'organe législatif est présumé agir en respectant les obligations contractées par le Canada lors de la signature de traités et conventions internationales. Le deuxième volet se rapporte au fait que l'organe législatif est présumé respecter les valeurs et les principes du droit international coutumier et conventionnel : Ruth SULLIVAN, « Sullivan and Driedger on the Construction of Statutes », 4e éd. Toronto: Butterworths, 2002, p. 422.

[479] Dans l'arrêt *Daniels c. White*, [1968] R.C.S. 517, à la p. 541, le juge Pigeon a écrit ce qui suit : [TRADUCTION] [I]l s'agit ici d'un cas où il y a lieu d'appliquer la règle d'interprétation selon laquelle le Parlement n'est pas censé légiférer de manière à violer un traité ou de quelque manière incompatible avec la courtoisie internationale ou les règles établies du droit international. Voir également les arrêts *Capital Cities Communications Inc. c. Canada (C.R.T.C.)*, [1978] 2 R.C.S. 141, p. 173 et *R.* c. *Hape*, *précitée*, note 478. La présomption s'applique également au droit international coutumier et aux obligations issues de traités. À cet égard, voir aussi les arrêts *Zingre* c. *La Reine*, [1981] 2 S.C.R. 392, 409-410 (par le juge Dickson) ; *Succession Ordon c. Grail*, [1998] 3 R.C.S. 437, par. 137 et *Schreiber c. Canada (Procureur général)*, [2002] 3 R.C.S. 269, 2002 CSC 62, par. 50.

BIBLIOGRAPHIE

TABLE DE LA LÉGISLATION

Textes canadiens

1. *Code civil du Québec*, L.Q., 1991, c. 64.
2. *Code criminel*, L.R.C. 1985, c. C-46.
3. *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1
4. *Loi constitutionnelle de 1867*, L.R.C. (1985), Appendice II, n° 5.
5. *Loi modifiant le Code criminel (responsabilité pénale des organisations)*, L.R.C. c. C-46.

Textes américains

1. *Communications Decency Act*: *Telecommunications Act* de 1996, Pub. L. No. 104-104, tit. V, 110 Stat. 56, 133-43 (1996) (codifié dans les sections de 47 U.S.C.).
2. *Digital Millenium Copyright Act*, Pub. L. No. 105-304, 112 Stat. 2860 (1998), en ligne sur: < http://www.eff.org/IP/DMCA/hr2281_dmca_law_19981020_pl105-304.html > (visité le 2 juillet 2007).

Textes français

1. *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique*, publiée au journal officiel de la République française n° 143 du 22 juin 2004.

Textes européens

1. Directive *2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur* (« directive sur le commerce électronique »), en ligne sur : < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:FR:HTML > (visité le 2 juillet 2007).

Textes internationaux

1. Accord ADPIC du 15 avril 1994, disponible en ligne sur : < http://www.wto.org/french/tratop_f/trips_f/t_agm0_f.htm > (visité le 13 juillet 2007).
2. *Convention de Berne pour la protection des œuvres littéraires et artistiques*, Acte de Paris du 24 juillet 1971, en ligne sur : < http://www.wipo.int/treaties/fr/ip/berne/trtdocs_wo001.html > (visité le 10 juillet 2007).
3. *Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe*, Rome, 4 novembre 1950, R.T.E. n° 5, 213 R.T.N.U. 222.
4. *Convention sur la cybercriminalité*, STE n° : 185, Budapest, 23 novembre 2001.
5. *Convention sur la cybercriminalité*, Rapport explicatif, par. 10, STE n° : 185, Budapest, 23 novembre 2001, Conseil de l'Europe, http://www.libertysecurity.org/IMG/pdf/ExplanatoryReportFr.pdf (visité le 22 mars 2009).
6. *Pacte international relatif aux droits civils et politiques des Nations Unies* adopté et ouvert à la signature, à la ratification et à l'adhésion par résolution de l'Assemblée générale n° 2200A (XXI) du 16 décembre 1966, R.T.C. 1976, n° 47, RTNU, vol. 999, n° 171.

7. *Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques*, Rapport explicatif, par. 8-9, STE n°: 185, Strasbourg, 28 janvier 2003, Conseil de l'Europe, http://www.inach.net/content/cctreatyaddexfr.html (visité le 22 mars 2009).
8. *Traité de l'Organisation Mondiale de la Propriété Intellectuelle sur le droit d'auteur*, CRNR/DC/94, Genève, 20 décembre 1996, en ligne sur : <http://www.wipo.int/edocs/mdocs/diplconf/fr/crnr_dc/crnr_dc_94.html > (visité le 22 mars 2009).

DOCTRINE

Monographie et recueils

1. BRUN B., « Le blogue : un équilibre délicat entre communication et responsabilité », dans Leg@l.TI, 2007, Éd. Yvon Blais.
2. CÔTÉ-HARPER, G., RAINVILLE, P et TURGEON, J., « Traité de droit pénal canadien », 4e éd., Les Éditions Yvon Blais Inc., Cowansville, 1998, 1458 p.
3. DE VILLERS, M.-E., « Multi dictionnaire de la langue française », 3e éd., Montréal, Québec Amérique, 1997, p. 802.
4. GIBSON, W., « Neuromancer », New York, Ace Books, 1984.
5. HOGG, P., *Constitutional Law of Canada*, vol. 1, 3rd éd. (Supplemented). Scarborough, Ont.: Carswell, 1992.
6. PARENT, H., « Traité de droit criminel », 2e éd., Les Éditions Thémis, Montréal, 2007, 683 p.
7. SAINT AUGUSTIN, *Retract.* I, 9. PL 32, 596. BA 12, 319, cité dans Thomas D'AQUIN, *Somme théologique*, t. 2, Paris, Éditions du Cerf 1997.
8. SULLIVAN, R., « Sullivan and Driedger on the Construction of Statutes », 4e éd. Toronto: Butterworths, 2002.
9. TISCHER, M. et JENNRICH, B., « La bible Internet expertise et programmation », Paris, Micro Application, 1997, 1545 p.
10. TRUDEL, P., F. ABRAN, K. BENYEKHLEF et S. HEIN, « Droit du cyberespace », Montréal, Éditions Thémis, 1997, 1296 p.

11. TRUDEL, P., F. ABRAN, « Droit de la radio et de la télévision », Montréal, Éditions Thémis, 1991, 1180 p.
12. TRUDEL P., « Les responsabilités dans le cyberespace » dans Les dimensions internationales du droit du cyberespace, collection Droit du cyberespace, Paris, Éditions UNESCO- Économica, 2000, p. 235-269.
13. TRUDEL P. et GÉRIN-LAJOIE, R, « La protection des droits et des valeurs dans la gestion des réseaux ouverts » dans : Centre de recherche en droit public (CRDP), Les autoroutes électroniques : usages, droit et promesses, Montréal, Éditions Yvon Blais, 1995, p. 324-325.
14. TRUDEL, P., « La responsabilité des acteurs du commerce électronique » dans Vincent GAUTRAIS, Droit du commerce électronique, Montréal, Éditions Thémis, 2003, p. 607-649.
15. VERBIEST T., « Commerce électronique : le nouveau cadre juridique : publicité, contrats, contentieux », Bruxelles, Éditions Larcier, 2004, 228 p.
16. VERBIEST T. et E. WÉRY, « Le droit de l'Internet et de la société de l'information », Bruxelles, Larcier, 2001, 648 p.

Articles spécialisés

1. BECKER, L. E., « The Liability of Computer Bulletin Board Operators for Defamation Posted by Others », (1989) 22 *Connectitut Law Review* 203-239.
2. BOULVARD, N., « *Etats-Unis* -Dérives sur Internet : immunité des fournisseurs d'accès », Expertises des systèmes d'information, n°218, Septembre 1998, en ligne sur : < http://www.celog.fr/expertises/1998/som0898/immunite0898.htm > (visité le 28 juin 2008).
3. CARON, C., « Contrefaçon et sites communautaires: état des lieux jurisprudentiel », Communication Commerce Électronique, n° 12, Décembre 2007, comm. 143.
4. CUTRERA, T. A. « Computer Networks, Libel and the First Amendment », (1992) 11 *Computer L.J.* 555-583.

5. DEVILLARD A, « Le monde Internet chahute la loi sur l'économie numérique », 19 février 2003, en ligne sur : < http://www.01net.com/article/201958.html > (visité le 25 juillet 2007).
6. DONOHUE, J. P., « Litigation in Cyberspace: Jurisdiction and Choice of Law –A United States Prespective », *American Bar Association, Subcommittee on International Transactions* (1997), 7.
7. FONDEVILLE, O. et JOUANNON, A.-S., « Le 'manifestement illicite', mystérieux point de rencontre entre la victime et l'hébergeur » Juriscom.net, 7-04-2008, en ligne sur : < http://www.juriscom.net/pro/visu.php?ID=1051 > (visité le 19 février 2009).
8. Forum des droits sur l'Internet, « États-Unis: extension du régime de responsabilité allégée aux agences matrimoniales virtuelles », en ligne sur : < http://www.foruminternet.org/specialistes/veille-juridique/actualites/tats-unis-extension-du-regime-de-responsabilite-allegee-aux-agences-matrimoniales-virtuelles.html > (visité le 20 janvier 2009).
9. Forum des droits sur l'Internet, « États-Unis : eBay déclaré non responsable des commentaires publiés par les internautes », en ligne sur : < http://www.foruminternet.org/specialistes/veille-juridique/actualites/tats-unis-ebay-declare-non-responsable-des-commentaires-publies-par-les-internautes.html > (visité le 16 février 2009).
10. Forum des Droits sur l'Internet, « Hyperliens : statut juridique », 3 mars 2003, en ligne sur : < http://www.foruminternet.org/telechargement/documents/reco-hyli-20030303.htm > (visité le 11 juin 2007).
11. Forum des droits sur l'Internet, Recommandation du Forum des droits sur l'internet « Les Enfants du Net (2) – Pédopornographie et pédophilie sur l'internet », 25 janvier 2005, en ligne sur : < http://www.foruminternet.org/specialistes/concertation/recommandations/recommandation-du-forum-des-droits-sur-l-internet-les-enfants-du-net-2-pedo-pornographie-et-pedophilie-sur-l-internet.html > (visité le 19 février 2009).
12. *Google*, condamné en tant qu'hébergeur de blog, Légalis.net, 17 décembre 2007, en ligne sur : < http://www.legalis.net/breves-article.php3?id_article=2117 > (visité le 26 janvier 2009).

13. GRATTON, É., « La responsabilité des prestataires techniques Internet au Québec », *Lex Electronica*, vol. 10, n° 1, Hiver 2004, en ligne sur : < http://www.lex-electronica.org/articles/v10-1/gratton.htm > (visité le 12 juin 2007).
14. GRAY, J. A., « Strict Liability for Dissemination of Dangerous Information? », 82 (1990) *Law Library Journal* 497.
15. HARDOUIN, R., « Observations sur les nouvelles obligations prétoriennes des hébergeurs », Juriscom.net, 08/11/2007, en ligne sur : < http://www.juriscom.net/uni/visu.php?ID=983 > (visité le 23 février 2009).
16. JOHNSON, David R. and MARKS, Kevin, « Mapping Electronic Data Communications Onto Existing Legal Metaphors: Should We Let Our Conscience (and our Contracts) Be our Guide? », (1993) 38 *Villanova L. Rev.* 487-515.
17. KEYES, J. M. et SULLIVAN, R., « A Legislative Perspective on the Interaction of International and Domestic Law », dans Oonagh E. Fitzgerald et al, *The Globalized Rule of Law*, Éditions Irwin Law, 2006, 660 p., en ligne sur : < http://www.ciaj-icaj.ca/english/publications/124Keyes-Sullivan%20_version%20francais_.pdf > (visité le 18 mars 2009).
18. KLEIN, G., « De la cybernétique à la cyberculture », *Le Monde, télévision, radio, multimédia*, 21, 22 janvier 1996.
19. LANHAM, D., « Complicity, Concert and Conspiracy », [1980] 4 *Crim. L.J.* 276.
20. Le Portail Société de l'Information Internet, « Loi pour la confiance dans l'économie numérique », en ligne sur : < http://www.internet.gouv.fr/information/information/dossiers/loi-pour-confiance-dans-economie-numerique-len/adoption-loi-pour-confiance-dans-economie-numerique-len-40.html > (visité le 20 juillet 2007).
21. Legalis.net, « Commentaire de l'ordonnance rendue par la "Northern District Court of California", le 21 novembre 1995, Religious Technology Center (Église de Scientologie) / Netcom, –Responsabilité d'un prestataire de services en ligne et de son fournisseur d'accès, en matière de contrefaçon commise par un abonné du prestataire », en ligne sur : < http://www.legalis.net/cgi-

iddn/french/affiche-jnet.cgi?droite=commentaires/comm_netcom_1195.htm > (visité le 28 juin 2007).

22. Legalis.net, « Wikipédia, hébergeur sans obligation », 8 novembre 2007, en ligne sur : < http://www.legalis.net/article.php3?id_article=2073 > (visité le 28 janvier 2009).
23. LOUNDY, D.J., « E-LAW 4: Computer Information Systems Law and System Operator Liability », (1998) 21 *Seattle University Law Review* 1075.
24. LOUNDY, D.J., « Holding the line, on-line, expands liability », (8 juin 1995) *Chicago Daily Law Bulletin* 6.
25. LUCAS, A., « La responsabilité civile des acteurs de l'Internet », (2001) *Auteurs & Media*, 42-52.
26. MAY, B., « Responsabilité des acteurs du web 2.0 : l'histoire sans fin », La Semaine Juridique Entreprise et Affaires n° 17, 24 avril 2008, 1540.
27. McDANIEL, J.R., « Electronic Torts and Videotext-At the Junction of Commerce and Communications », *Rutgers Computer & Technology Law Journal*, n° 18, 1992, p. 773 et 823.
28. NEUSTADT, R.M., SKALL, G.P. and HAMMER, M., « The regulation of electronic publishing », *Federal Communications Law Journal*, n° 33, 1981, p. 331-332.
29. Office québécois de la langue française, *Le grand dictionnaire terminologique*, < http://www.granddictionnaire.com > (visité le 27 janvier 2009).
30. PERRITT Jr., H. H., « Tort liability, the first amendment and equal access to electronic networks », (1992) 5 *Harvard Journal of Law & Technology*, 65-151.
31. PERRITT Jr., H. H., « Computer crimes and torts in the global information infrastructure: intermediaries and jurisdiction », 12 octobre 1995.
32. POULLET, Y. et THUNIS, X., « Droit et informatique: un mariage difficile » dans *Computers and Telecommunications: Is There a Lawyer in this Room?,* Namur, E.Story-Scientia, 1987.
33. RENAUD, P., VERBIEST, T. et VANDEVELDE, B., « Le Web 2 dans l'entreprise: quelle responsabilité », 14 février 2008, en ligne sur : <

http://www.droit-technologie.org/dossier-165/le-web-2-0-dans-l-entreprise-quelle-responsabilite.html > (visité le 19 janvier 2009).

34. SCHLACHTER, E., « Cyberspace, the Free Market and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions », (1993) 16 *Hastings Comm/Ent L.J.* 113.
35. SPOOR, J.H., « Database Liability: Some General Remarks », (avril 1989) 3 *International Computer Law Adviser 4.*
36. STROWEL, A. et N. IDE, « Responsabilités des intermédiaires : actualités législatives et jurisprudentielles », dans *Droit Nouvelles technologies*, en ligne sur : < http://www.droit-technologie.org/2_1.asp?dossier_id=32 > (visité le 2 juillet 2007).
37. TAÏEB, J., « Prestataires techniques de l'Internet : le sens des responsabilités », Juriscom.net, en ligne sur : < http://www.juriscom.net/pro/visu.php?ID=1066 > (visité le 22 janvier 2009).
38. THOUMYRE, L., « La responsabilité pénale et extra-contractuelle des acteurs de l'Internet », Lamy, droit des médias et de la communication, juin 2007, étude 464.
39. THOUMYRE, L., « L'art et la manière de notifier l'hébergeur 2.0 », Études n° 5, Communication Commerce Électronique, février 2008.
40. THOUMYRE, L., « Précisions contrastées sur trois notions clés relatives à la responsabilité des hébergeurs », Revue Lamy droit de l'immatériel, février 2008, n. 35, p. 18.
41. TRUDEL, P., « La responsabilité sur Internet », juillet 2002, *Revue Droit & Toile.*
42. TRUDEL, P., « La responsabilité civile sur Internet selon la Loi concernant le cadre juridique des technologies de l'information » dans Service de la formation permanente, Barreau du Québec, *Développements récents en droit de l'Internet*, Cowansville, Éditions Yvon Blais, 2001, 107-141, en ligne sur : « http://www.crdp.umontreal.ca/cours/drt6929f/Resp.%20civile-int.fpbq11-01.pdf » (visité le 18 juin 2007).
43. TRUDEL, P., « La responsabilité sur Internet en droit civil québécois », en ligne sur:

< http://www.chairelrwilson.ca/documents/TRUDEL_resp_internet.pdf > (visité le 5 janvier 2009).

44. THOREL, J., « LCEN: le SNEP désapprouve en partie l'avis du Conseil Constitutionnel », Zdnet.fr, 22/06/2004, en ligne sur : < http://www.zdnet.fr/actualites/telecoms/0,39040748,39157926,00.htm > (visité le 19 février 2009).
45. TROIANO, M. A., « Comments –The New Journalism? Why the Traditional Defamation Laws Should Apply to Internet Blogs? », (2007) 56 *American University Law Review* 1450, en ligne sur: < http://www.wcl.american.edu/journal/lawrev/55/troiano.pdf?rd=1 > (visité le 21 juin 2008).
46. TRUDEL, P., « Quel droit et quelle régulation dans le cyberespace? », en ligne sur : < https://papyrus.bib.umontreal.ca/jspui/bitstream/1866/57/1/0042.pdf > (visité le 1er janvier 2008).
47. TRUDEL, P., « L'exercice de la liberté d'expression dans le cyberespace : le défi d'assurer l'application effective des droits proclamés », en ligne sur : < http://64.233.169.104/search?q=cache:5AZLcz-TPM4J:www.unesco.org/comnat/france/Colloque_liberte_expression_2002/P_Trudel.pdf+lex+electronica+le+germe+de&hl=fr&ct=clnk&cd=6&gl=ca > (visité le 7 janvier 2008).
48. TRUDEL, P., « Responsabilités des blogues » dans le cadre de la Conférence « Droit 2.0 : droit et web 2.0 », 20 avril 2007, en ligne sur : https://papyrus.bib.umontreal.ca/jspui/handle/1866/1322 > (visité le 7 janvier 2008).
49. VAN ERT, G., « Using international law in Canadian courts », 2002 *Kluwer Law International,* p. 99-100.
50. VIVANT, M., « La responsabilité des intermédiaires de l'Internet » JCP (G) 99 I p. 2021.
51. WEBER, A. M., « Annual Review of Law and Technology: VIII. Foreign & International Law: A. Cyberlaw: Cybercrime: The Council of Europe's Convention on Cybercrime », (2003) 18 *BERKELEY TECH. L.J.* 425-446.

52. WÉRY, E., « La notion de contenu manifestement illicite soumise au juge des référés », 15/02/2007, en ligne sur : < http://www.droit-technologie.org/actuality-1008/la-notion-de-contenu-manifestement-illicite-soumise-au-juge-des-refere.html > (visité le 19 février 2009).

Thèses et mémoires de maîtrise

1) GUILLEMARD, S., « Le droit international privé face au contrat de vente cyberspatial », Thèse de doctorat, Faculté des études supérieures, Université Laval, Québec, janvier 2003.
2) HOUDE, L., « Internet et le paradigme juridictionnel », Mémoire de maîtrise, Faculté des études supérieures, Université de Montréal, Québec, juin 2003.

Documents et rapports officiels

1) Conseil de l'Europe, *Le secrétaire général du Conseil de l'Europe : « Le but est d'harmoniser les législations pénales »*, http://www.coe.int/t/f/com/dossiers/interviews/20020309_InterviewSGLiberation.asp#P11_996 (visité le 10 juillet 2007).
2) Conseil National du crédit et du titre, « Problèmes juridiques liés à la dématérialisation des moyens de paiement et des titres », Paris, Banque de France, 1997.
3) COOK, R. J et KELLY, L. M., « La polygynie et les obligations du Canada en vertu du droit international en matière de droits de la personne », Ottawa, Canada, Section de la famille, des enfants et des adolescents, ministère de la Justice du Canada, septembre 2006, en ligne sur : < http://www.justice.gc.ca/fra/min-dept/pub/poly/index.html#01 > (visité le 18 mars 2009).
4) Europa, Activités de l'Union européenne –Synthèse de la législation, « Aspects juridiques du commerce électronique (« directive sur le commerce électronique ») », en ligne sur: < http://europa.eu/scadplus/leg/fr/lvb/l24204.htm > (visité le 18 juillet 2007).
5) Ministère de la Justice du Canada, « Le Canada signe une entente internationale en vue de lutter contre les crimes racistes sur Internet », 8 juillet

2005, en ligne sur : < http://www.justice.gc.ca/fra/nouv-news/cp-nr/2005/doc_31572.html > (visité le 10 juillet 2007).

6) Ministère de la Justice du Canada, « Résumés des mémoires présentés dans le cadre de la consultation sur l'accès légal », 6 août 2003, en ligne sur : < http://www.justice.gc.ca/fra/cons/al-la/res-sum/index.html > (visité le 19 mars 2009).

7) *NIIAC Recommendation (December 12, 1995) to Secretary Ron Brown Regarding Content Regulation*, en ligne sur :< http://www.niiac-info.org/~niiac/content.html > (visité le 11 février 2009).

8) RACICOT, M., M. S. HAYES, A. R. SZIBBO et P. TRUDEL, « The Cyberespace is not a «No Law Land», A Study of the Issues of Liability for Content Circulating on the Internet », Ottawa, Industrie Canada, Février 1997, 306 p.

9) Rapport d'information n° 627 sur la mise en application de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, présenté le 16 avril 2008 par les députés M. Jean Dionis du Séjour et Mme Corinne Erhel, p. 16, en ligne sur le site de l'Assemblée Nationale : < http://www.assemblee-nationale.fr/13/rap-info/i0627.asp (visité le 11 février 2009).

10) TRUDEL, P. et BENYEKHLEF, K., « Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes », Mémoire présenté à la Commission de la Culture de l'Assemblée Nationale dans le cadre de son mandat sur l'étude du rapport quinquennal de la Commission d'accès à l'information, Montréal, Centre de Recherche en droit public, Université de Montréal, 1997, p. 24 : en ligne sur: < https://papyrus.bib.umontreal.ca/dspace/bitstream/1866/71/1/0072.pdf > (visité le 22 juin 2008).

TABLE DE JURISPRUDENCE

Canada

1. *Canada (Citoyenneté et Immigration)* c. *Khosa*, 2009 CSC 12 (CanLII).

2. *Capital Cities Communications Inc. c. Canada (C.R.T.C.)*, [1978] 2 R.C.S. 141.
3. *Daniels c. White*, [1968] R.C.S. 517.
4. *Egan c. Canada*, [1995] 2 R.C.S. 513.
5. *Irwin Toy Ltd. c. Québec (Procureur général)*, [1989] 1 R.C.S. 927.
6. *R.* c. *Anderson* [1990] 1 R.C.S. 265.
7. *R.* c. *Chartrand*, [1994] 2 R.C.S.864 *R.* c. *Chartrand*, [1994] 2 R.C.S.864.
8. *R.* c. *Greyeyes*, [1997] 2 R.C.S. 825, 8 C.R. (5th) 308, 116 C.C.C. (3d) 334.
9. *R.* c. *Hape*, [2007] 2 R.C.S. 292, 2007 CSC 26.
10. *R. c. Morgentaler*, [1993] 3 R.C.S. 463.
11. *R.* c. *P. (V.L.)*, [1993] 1 R.C.S. 837.
12. *R.* c. *Perka*, [1984] 2 R.C.S. 232.
13. *R.* c. *Théroux*, [1993] 2 R.C.S. 5.
14. *R.* c. *Twigge (H.)*, (1996) 148 Sask. R. 254, 264-265 (C.A.).
15. *Schreiber c. Canada (Procureur général)*, [2002] 3 R.C.S. 269.
16. *Succession Ordon c. Grail*, [1998] 3 R.C.S. 437.
17. *Zingre* c. *La Reine*, [1981] 2 S.C.R. 392.

États-Unis

1. *Batzel v. Smith,* 333 F.3d 1018 (9th Cir. 2003).
2. *Carafano* c. *Metrosplash.com Inc.*, 207 F. Supp. 2d 1055, 1065-66 (C.D. Cal. 2002).
3. *Doe* c. *MySpace*, No. 1:06-cv-00983-SS (W.D. Tex 2007).
4. *Fair Housing Council of San Fernando Valley* c. *Roommate.com*, LLC, CV-03-09386-PA (9th Cir. May 15, 2007).
5. *Gentry v. eBay, Inc.*, 99 Cal. App. 4th 816, 830 (2002).
6. *Hellar* c. *Bianco*, 11 Cal. App. 2d 424 P.2d 757, 28 ALR2d 451 (1952).
7. *Kenneth M. Zeran* v. *America Online, Inc.*; U.S. District Court, E.D. Virginia, 958 F.Supp. (1997); U.S Court of Appeals, 4th Circuit, CA-96-1564-A, 129 F.3d 327 (1997); 118 S. Ct. 2341 (1998), rejeté.
8. *Religious Technology Center* v. *Netcom Online Communication Services Inc.*, 907 F. Supp. 1361 (N.D. Cal.1995).

9. *Reno, Attorney General of the United States, et al.* v. *American Civil Liberties Union (ACLU) et al.*, 117 S.Ct. 2329, 138 L.Ed.2d 874 (1997), en ligne sur : < http://supct.law.cornell.edu/supct/html/96-511.ZO.html > visité le 16 février 2009).
10. *Scott* c. *Hull*, 22 Ohio App.2d 141, 259 N.E.2d 160, (1970).
11. *Schneider v. Amazon.com, Inc.*, 31 P.3d 37, 39 (Wash.Ct.App. 2001).
12. *Stratton Oakmont, Inc.* v. *Prodigy Services Co.*, 23 Med L.R. 1794 (N.Y. Sup. Ct. 1995).
13. *Tackett* c. *General Motors Corporation*, 836 F.2d 1042 (7th Cir. 1987).
14. *Woodling* c. *Knickerbocker*, 17 N.W. 387 (Minn. 1883).

France

1. *Affaire Polac*, TGI Paris, 29 janvier 1986, D. 1986, flash n° 10.
2. Alain Afflelou c/ Google, Free, Tribunal de grande instance de Paris, Ordonnance de référé du 27 février 2006, en ligne sur Legalis.net : < http://www.legalis.net/jurisprudence-decision.php3?id_article=1648> (visité le 19 février 2009).
3. *Comité de défense de la cause arménienne* c/ *M. Aydin S.*, TGI de Paris, 15 novembre 2004, et Cour d'Appel de Paris, 8 novembre 2006, France Télécom services de communication résidentiels.
4. *Décision du Conseil Constitutionnel* du 10 juin 2004, n°2004-496, en ligne sur le site du Conseil Constitutionnel: < http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/depuis-1958/decisions-par-date/2004/2004-496-dc/decision-n-2004-496-dc-du-10-juin-2004.901.html > (visité le 19 février 2009).
5. *Google* c/ *Zadig productions*, TGI Paris, 19 octobre 2007, Juris-Data n°2007-344344, RDLI 2007/32 n°1062 obs. Costes L.
6. *Google* c/ *Flach Films*, Tribunal de commerce de Paris, 8ème chambre, Jugement du 20 février 2008, en ligne sur : < http://www.legalis.net/jurisprudence-decision.php3?id_article=2223 > (visité le 19 février 2009).

7. *Google Inc* c./ *Benetton, Bencom*, Cour d'appel de Paris, 14 ième chambre, section A, Arrêt du 12 décembre 2007, en ligne sur : < http://www.legalis.net/jurisprudence-decision.php3?id_article=2116 > (visité le 26 janvier 2009).
8. *Groupe Mac.* c./*Gilbert D*, TGI Lyon, 14e Ch., 21 juillet 2005.
9. *Jean-Yves L. dit LAFESSE / Myspace*, TGI de Paris, Ordonnance de référé 22 juin 2007, en ligne sur : Legalis.net, < http://www.legalis.net/jurisprudence-decision.php3?id_article=1965 > (visité le 21 janvier 2009).
10. *Jean-Yves Lafesse* c. *Dailymotion*, TGI Paris, 3ème chambre, 1ère section, 15 avril 2008, en ligne sur : <http://www.juriscom.net/jpt/visu.php?ID=1057 > (visité le 2 mars 2009).
11. *Lacoste* c. *SA Multimania Production et a.*, TGI Nanterre, 1er ch. A., 8 décembre 1999, J.C.P. 2000.II.102.
12. *Lehideux et Isorni c. France*, arrêt du 23 septembre 1998, *Recueil des arrêts et décisions* 1998-VII.
13. *Les Arnaques.com* c / *Ed. régionales de France*, CA de Versailles, 12 décembre 2007.
14. *Marianne B. et autres* c./ *Wikimedia Foundation*, Tribunal de grande instance de Paris, Ordonnance de référé 29 octobre 2007, en ligne sur : < http://www.legalis.net/jurisprudence-decision.php3?id_article=2071> (visité le 28 janvier 2009).
15. *Mme M. B., M. P.T., M. F .D.* c/ *Wikimedia Foundation Inc.*, TGI de Paris, référé, 29 octobre 2007, en ligne sur : < http://www.juriscom.net/jpt/visu.php?ID=980 > (visité le 19 février 2009).
16. *M. Olivier Dahan* c/ *M. Éric Duperrin*, TGI Nanterre, 28 février 2008, Juriscom.net, en ligne sur : < http://www.juriscom.net/jpt/visu.php?ID=1031> (visité le 22 janvier 2009).
17. *M. O. D.* c/ *SARL Planète Soft*, TGI Nanterre, 7 mars 2008, Juriscom.net, en ligne sur : < http://www.juriscom.net/jpt/visu.php?ID=1035 > (visité le 22 janvier 2009).
18. *Monsieur Omar Sy et Monsieur Fred Testot et autres* c/ *S.A. Dailymotion*, TGI de Paris, 15 avril 2008.

19. *Olivier Martinez* c./ *Bloobox Net*, TGI Paris, 26 mars 2008, Juriscom.net, en ligne sur : < http://www.juriscom.net/jpt/visu.php?ID=1043 > (visité le 22 janvier 2009).

20. *SARL Lycos France* c./ *Abdelhadi S. et SA et SAS iEurope, CA Paris, 6 juin 2007, en ligne sur :* < *http://www.lasic.fr/public/cspla/36.pdf* > (visité le 19 février 2009).

21. *Yahoo (UEJF et Licra* c. *Yahoo ! Inc. et Yahoo France*, TGI Paris, réf., 22 mai 2000, Comm. com. électr.2000. comm. n°92, note J-Chr. GALLOUX ou en ligne : Revue du droit des technologies de l'information < http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm> (visité le 8 juin 2007).